NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INFORMATION ASSURANCE AS A SYSTEM OF SYSTEMS IN THE SUBMARINE FORCE

by

Mark R. Morgan

September 2013

Thesis Advisor:	Rex Buddenberg
Second Reader:	Walter E. Owen

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE INFORMATION ASSURANCE AS A SYSTEM OF SYSTEMS IN THE SUBMARINE FORCE			**5. FUNDING NUMBERS**
6. AUTHOR(S) Mark R. Morgan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ______N/A______.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

There are significant gaps in the United States Navy Submarine Force's ability to integrate and manage Information Assurance requirements (IA), Information Technology (IT) manpower, End-to-End security, IT equipment, IT training, and applicable documentation that meet the intent of the "Design for Undersea Submarine Warfare" initiative promulgated in July 2011.

Furthermore, the Submarine Force lacks common criteria for IA integration as a system of systems. IT operators and system administrators must understand the concept of end-to-end security. Senior leadership should understand the end-to-end security concept so as to understand the cause and effect on overall ship mission and vulnerabilities.

Organizational governance must raise the level of awareness as to network security protection. Training, personnel, and equipment, should connect with ethics and security practices for total End-to-End Security. A paradigm shift in watchstanding must take place. Information Technician Submarines (ITS) duties are no longer a collateral duty. Submarine communications division and ITS division merging has the potential to solve the manning and watchstanding challenges. Senior enlisted leadership and senior communications officer leadership should take the lead on this merger, with command and control element support.

Military procurement system is more oriented on acquiring platforms, not cross-platform sections. A more cohesive interface between the TYCOMS and the acquisition corps is needed.

14. SUBJECT TERMS Information Assurance, IA, New Design for Undersea Warfare, System of Systems, End-to-End Security, Information Assurance Boundaries, Information Technician Submarines, Risk Assessment, CYBER-1, Limited Duty Officer			**15. NUMBER OF PAGES** 133
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

INFORMATION ASSURANCE AS A SYSTEM OF SYSTEMS IN THE SUBMARINE FORCE

Mark R. Morgan
Lieutenant, United States Navy
B.S., Electronics and Management,
Southern Illinois University Carbondale

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Mark R. Morgan

Approved by: Rex Buddenberg
Thesis Advisor

Walter E. Owen
Second Reader

Clifford A. Whitcomb
Chair, Systems Engineering Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There are significant gaps in the United States Navy Submarine Force's ability to integrate and manage Information Assurance requirements (IA), Information Technology (IT) manpower, End-to-End security, IT equipment, IT training, and applicable documentation that meet the intent of the "Design for Undersea Submarine Warfare" initiative promulgated in July 2011.

Furthermore, the Submarine Force lacks common criteria for IA integration as a system of systems. IT operators and system administrators must understand the concept of end-to-end security. Senior leadership should understand the end-to-end security concept so as to understand the cause and effect on overall ship mission and vulnerabilities.

Organizational governance must raise the level of awareness as to network security protection. Training, personnel, and equipment, should connect with ethics and security practices for total End-to-End Security. A paradigm shift in watchstanding must take place. Information Technician Submarines (ITS) duties are no longer a collateral duty. Submarine communications division and ITS division merging has the potential to solve the manning and watchstanding challenges. Senior enlisted leadership and senior communications officer leadership should take the lead on this merger, with command and control element support.

Military procurement system is more oriented on acquiring platforms, not cross-platform sections. A more cohesive interface between the TYCOMS and the acquisition corps is needed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADNS	Automated Digital Network System
ARPNET	Advanced Research Projects Agency Network
ATO	Authority To Operate
BA	Billets Authorized
BBS	Bulletin Board System
C&A	Certification and Authorization
CAC	Common Access Card
CBT	Computer Based Training
CCE	Contact Center Enterprise
CEH	Certified Ethical Hacking
CISSP	Certified Information Security Professional
CJCS	Chairman Joint Chiefs of Staff
CO	Commanding Officer
COMNAVCYBERFOR	Commander Navy Cyber Force
COMNAVNETWARCOM	Commander Navy Network Warfare Command
COMPOSE	Common Personal Computer Operating System Environment
COMTENTHFLEET	Commander Tenth Fleet
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CSI	Cyber Security Inspection
CSIP	Cyber Security Inspection and Certification Program
COMSUBLANT	Commander Submarine Force Atlantic
COMSUBPAC	Commander Submarine Force Pacific
CSRR	Common Submarine Radio Room
CTO	Computer Tasking Order
CWO	Chief Warrant Officer
DHRA	Defense Human Resources Activity
DICAP	Department of Defense Information Assurance Certification and Accreditation Program
DiD	Defense In Depth
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIIS	DoD Intelligent Information System
DoN	Department of the Navy
DUSW	Design for Undersea Warfare
ECM	Enlisted Community Manager

ECS	Exterior Communications Subsystem
ET	Electronics Technician
FCC	Fleet Cyber Command
FFO	First in First Out
FISMA	Federal Information Security Management act
FT	Fire Control Technician
GCCS-M	Global Command and Control System-Maritime
GENSER	General Service
GIG	Global Information Gig
HBSS	Host Based Security System
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IARM	Information Assurance Risk Management
IAVA	Information Assurance Vulnerability Assessment
IAVM	Information Assurance Vulnerability Management
IAWF	Information Assurance Workforce
IS	Information Systems
ISIC	Immediate Superior in Command
ISO	International Standards Organization
IT	Information Technology
ITS	Information Technician Submarines
JNET	Journeyman Network
LAN	Local Area Network
LDO	Limited Duty Officer
LOE	Lines of Effectiveness
NAVADMIN	Navy Administration
NCF	Navy Cyber Forces
NCTAMSPAC	Naval Computer and Telecommunications area Master Station Pacific
NEC	Navy Education Code
NIPRNET	Non-secure Internet Protocol Router Network
NIST	National Institute of Technology
NMCI	Navy and Marine Corps Internet
NMP	Navy Manpower Plan
NSA	National Security Agency
NSVT	Network Security Vulnerability Technician
NTCSS	Naval Tactical Command Support System
NTDPS	Non Tactical Data Processing Subsystem

OCA	Office of Assessment and Compliance
OCONUS	Outside Continental United States
OCRS	Online Compliance Reporting System
ONE-NET	Outside Continental United States Navy Enterprise Network
OPNAVINST	Operational Naval Instruction
OPTEMPO	Operational Tempo
OSI	Open Systems Interconnection
PCS	Permanent Change of Station
PED	Personal Electronic Device
PIA	Privacy Impact Statement
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PM	Program Manager
PMS	Preventive Maintenance System
PTS	Perform to Serve
S/MIME	Secure Multiple Internet Mail Extensions
SIPRNET	Secure Internet Protocol Router Network
SME	Subject Matter Expert
SOS	System of Systems
SRB	Selective Reenlistment Bonus
SSAA	System Security Authorization Agreement
SSBN	Submerged Ship Ballistic Nuclear
SSH	Secure Shell
SSL	Secure Socket Layer
SSN	Submerged Ship Nuclear
STDA	Submarine Tactical Display Auxiliary
SUBLAN	Submarine Local Area Network
SUBSAFE	Submarine Safety
SWFTS	Submarine Warfare Tactical System
TACLAN	Tactical Local Area Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS T	Transport Layer Security
TS-SCI	Top Secret-Special Compartment Information
TYCOM	Type Commander
USB	Universal Serial Bus
USG	United States Government Network
USN	United States Navy
UWLAN	Unclassified Wireless Local Area Network
VLF	Very Low Frequency

VOIP	Voice Over Internet
VTE	Virtual Training Environment
WAN	Wide Area Network

EXECUTIVE SUMMARY

The submarine Information Technician Submarines (ITS) rating is in its infancy. Support in the form of equipment training and personnel is, too. Similarly, the understanding of end-to-end security and information assurance requirements management is also in its infancy. The new IT is rating is in charge of maintaining submarine networks from unclassified to top secret special compartment information and higher. These networks are the "other combat system" and must be treated as such. In order for the afloat command and control element to manage this other combat system like all other systems on submarines, commanding officers expect support infrastructure for proper training, equipment, and personnel. Unlike other systems onboard, and due to the networks autonomous nature at times, the submarine network(s) require a certain level of information assurance and end-to-end security due to the submarine networks ability to reach off hull like a virtual brow that can allow anything to cross- this can be a significant security risk making our submarines externally vulnerable. This external threat is not alone. Internal threat on board our submarines is primarily from of poor level of knowledge at the system administrator level and poor level of knowledge of information assurance requirements management at the executive level.

Quality sailors manage our onboard networks, like the rest of our systems on board the submarine. Allowing anything less, places the ship into inherent risk every time it is plugged into the global information gig. Not every sailor who volunteers or gets volunteered to be a submarine ITS should be doing that job. Scrutiny of personnel to manage our onboard networks should be held to a high standard. What makes the ITS rate different from the Information Technician (IT) rate in the rest of the Navy? Why does the submarine community need to spawn a separate rate? This question should bring forth two separate possibilities; (1) The rest of the Navy has not managed the IT rate enough that the submarine force had to set up a separate rate or (2) low personnel numbers in submarine manning requires greater versatility from each petty officer. Can the submarine force save money and use the stock IT rate or force the multi-capability farther down the organizational hierarchy?

There are few qualified leadership positions at the ISIC level and above to assist submarines with information assurance management. Force shaping at the Limited Duty Officer level and procurement of a new Information Systems Submarine Chief Warrant Officer level will invest in permanent manpower relief.

After three years of the creation of the ITS rate, only now in 2013 is there an official ITS training pipeline. Unlike other systems on board a submarine that have a tendency to remain somewhat static, networking and all that it implies will remain fluid from the DoD level down to the deck plate. It is still up to the afloat command to train the majority of their ITS personnel for the next few years. Leaders must demand nothing less than top-notch on-board training. If personnel are not training themselves or new personnel are not being trained via the official ITS training pipeline for equipment on board, then detailed feedback on the external supplied training must be swift and clear.

Submarine networking equipment follows the standard program of record acquisition process. Fleet feedback from afloat platforms is crucial to improving the network systems and system of systems for proper interoperability to meet capability.

Guidance at all levels from various organizations creates myriad instructions, technical manuals, and messages from operational organizations to defense contracting program managers. Commanding officers currently do not know what they are supposed to know -this continues to be a problem. The number of personnel to properly manage this continuously changing guidance are few, but increasing slowly. Managing the sea of guidance should not be left up to the afloat unit alone. There is a better solution that involves continuous feedback from onboard and iterations of guidance until a mature product supports submarine.

The Navy procurement and acquisition process, specifically test evaluation and design review, must be fully understood by senior leadership other than those involved directly with defense acquisition as a program manager or a liaison for TYCOM. The checks and balances between program growth versus military needs and requirements are insufficient in preventing adequate efficiency before achieving effectiveness. The relationship between acquisition leadership and TYCOM is more of a dichotomy- split

and non-overlapping. A more cohesive connection needs to be made between TYCOM and the procurement and acquisition leadership.

End-to-end security strengthening of our information assurance is the goal. End-to-end security parallels the end-to-end reliability mechanisms so elegantly implemented in the Internet, specifically transmission control protocol (TCP). Without reaching this goal, the management and employment of our networks is inherently at risk. IT operators and system administrators must understand the concept of end-to-end security so as to put in place necessary measures for a proper end-to-end security model. Senior leadership should understand the end-to-end security concept so as to understand the cause and effect on overall ship mission and support functions. Network operation, security, and administration are no longer a collateral duty. Treating it as such prevents long-term investment in strengthening our information assurance and end-to-end security across the virtual brow—there is a better solution.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is not necessarily for the submarine communications and IT/LAN division personnel, but more for their leadership. Thank you to the sailors on board for their input. Special thanks to Rex Buddenberg for his technical experience, insight, and sea stories that always seem to have a learning point behind them. Appreciation goes to Mary Vizzini for her online teachings and for putting up with my barrage of questions. Thanks to Dr. Wally Owen for volunteering to be my second reader when nobody else would. Special call goes out to Mike Aquila for helping take my concepts and transforming them into custom graphics. Finally, a hearty thank-you to all of the PD-21 distance learning, library, TAC, and all of the staff working behind the scenes. Working full-time in two different submarine squadrons and going back to school was difficult but the staff took care of any and every process allowing our class to fully concentrate on learning. As we say on the boat, when the job is done, "surface surface surface!"

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

There are significant gaps in the United States Navy (USN) Submarine Force's ability to integrate and manage Information Assurance requirements (IA), Information Technology (IT) manpower, End-to-End security, IT equipment, IT training, and applicable documentation that meets the intent of the "Design for Submarine Warfare" initiative promulgated in July 2011. The DUSW's intent is to have a shared sense of main objectives, and to align multiple efforts" (Caldwell, Richardson and Breckenridge 2011).

Furthermore, the Submarine Force lacks common criteria for IA integration as a system of systems (SoS), when such an SoS is defined as a structured methodology to standardize and document IA requirements, IT requirements management, IT manpower, end-to-end security paralleled with end-to-end reliability, IT equipment and training, IA physical/functional/behavioral network boundaries, and applicable documentation that meets the intent of the "New Design for Submarine Warfare" initiative.

This thesis presents an analysis of the current position and possible solutions for the Submarine Force to properly and effectively institutionalize, at the Type Commander (TYCOM) and afloat command level, IA integration as an SoS with an understanding of End-to-End security across all platform architectures and vertically from the most junior submarine IT workforce personnel to afloat Commanding Officer, Major Commander, Type Commanders (TYCOM) and sponsored Program Managers (PM). These solutions are currently available and able to be implemented without significant impact to the Submarine Fleet budget, manpower, or networks.

In this thesis, the introduction of a new concept representation of "information assurance trade-space" will be used. It encompasses not only the generally accepted definition of IA but also includes the additional elements of training, personnel, and equipment. Figure 1 depicts a visual representation of this new concept or representation.

Of note: Cyber is an overused term with multiple meanings. Readers of this thesis are encouraged to think of the term "Cyber" as something a little more analogous to "network centric." Additionally, tackling improving information systems security is more of a systems function. To address improving information security is more of a personnel and policy function.

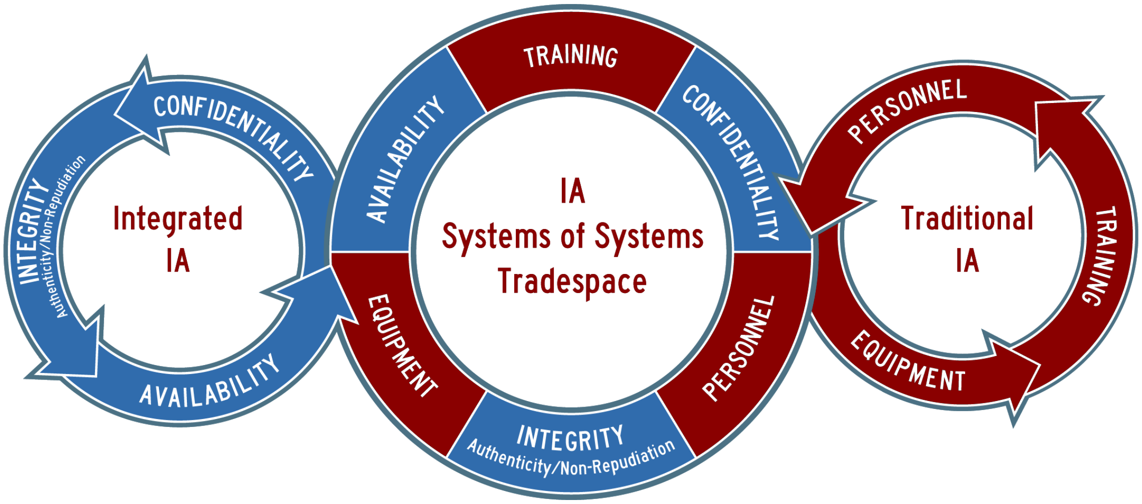

Figure 1. Information Assurance Tradespace

B. RESEARCH QUESTIONS

The research will address the questions of "How can the Submarine Force better prepare and improve its Information Technician (IT) personnel, equipment, and training to meet increasing submarine warfare requirements worldwide? How can this be accomplished while employing undersea forces and delivering future undersea warfighting capabilities without further unnecessarily sacrificing valuable monetary and manpower resources?"

Furthermore, this research will analyze the capability of the Submarine Force's "New Design for Undersea Warfare" (DUSW) initiative, described as the ability to "fight our virtual ship in the cyber domain as capably as we do in the undersea domain" (Caldwell and Richardson 2011, 4).

The aim of this research is to provide submarine combatant commanders, submarine type commanders, submarine squadron commodores, and submarine afloat commanding officers with an improved comprehension of the concepts necessary for the Submarine Force's ability to fight the virtual ship in the cyber domain as capably as the undersea domain. The term *virtual ship* should not imply improved information systems but rather a comparison of warfare in a physical battle space of ether land, air, or sea with the virtual concept of network warfare.

C. DEFINITIONS AND DOCUMENTATIONS OF INFORMATION ASSURANCE

Information Assurance (IA) is a phrase that is often used and equally misunderstood. As the term IA matured over the years, technology has become younger and more advanced. In other words, new technology is emerging so fast it is slow to mature. Since the subject of this thesis is IA as a system of systems in the submarine force, it is appropriate to address the basics of what generally has been adopted as the definition and understanding of IA. In addition to a basic definition, some of the multiple meanings and definitions IA has taken on over the past decade will also be discussed. Currently, the Defense Information Systems Agency (DISA) website alone maintains 338 line items under their policy guidance webpage that have some form of connection with IA or information security (DISA website 2012). It is with no surprise that all Echelon Commands levels may not fully understand or be able to keep up with policy guidance pertaining to IA and all that it entails.

A generally accepted definition of IA is provided in the Chairman Joint Chiefs of Staff Joint Publication 1–02 as measures that "protect and defend information and information systems by ensuring: availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (CJCS JP1–02 2013, 137).

D. DEFENSE IN DEPTH AND INFORMATION ASSURANCE

"IA is achieved when information and information systems are protected against such attacks through the application of security services" (NSA IA Group, 2013). Overall, the concept of IA includes the measures that protect and defend information and information systems by ensuring integrity, authentication, availability, confidentiality, and non-repudiation. A closer review shows IA broken down into two parts; protection of the information itself (authenticity and confidentiality) and protection of the information system infrastructure (integrity and availability). It is important to understand that protections of the infrastructure alone may have little benefit to protecting the information. In parallel, there are measures to protect the information (data) and measures to protect the information system (infrastructure); the protection measures for each are generally different. These same measures, or capabilities, of these services should allow for the defense of information systems by incorporating protection, detection, and reaction capabilities. In other words, in addition to incorporating protection mechanisms, Echelon Two and below commands need to expect vulnerabilities and include attack detection tools, policies, procedures, and training that allow them and their IT personnel to prepare, react, and recover from these attacks. In other words, what is necessary are solid personnel, readiness information management programs at the unit level. This layered approach towards people, technology, and operations is also known as "Defense in Depth" IA strategy (NSA IA Group 2013) , which will be covered in this thesis.

DoD Personnel and Readiness Information Management (P&R IM 2012) IA role is to offer guidance and training in the areas of:

- The Department of Defense Information Assurance Certification and Accredition Program (DIACAP). This provides oversight to and/or manages the C&A (Certification and Authorization) process on Defense Human Resources Activity (DHRA) components' information systems.
- Employee awareness training: This covers basic IA principles, security threats, risks, physical security, and so on.
- Information Assurance Vulnerability Management (IAVM). This includes producing required documentation, ensuring timely reporting of compliance statistics for each Information Assurance Vulnerability Alert (IAVA) and aggreatating compliance reports.

- Privacy Impact Assessments (PIAs): This includes evaluations of the privacy impact of any substantially revised or new IT systems that collect, maintain, or disseminate PII (Personnal Identifable Information) and for those systems or
- projects that convert PII paper-based records to electronic systems.

(P&RIM 2012)

The DoD IA Portal website is the one-stop-shop for Information Assurance Support Environment (DISA website 2012). IA may be a focal point for the Defense in Depth strategy, but policy addressing Information Assurance is different at every tier echelon level. For example, Information Assurance is part of the title in nine different DOD 8500 series instructions on the iase.disa.mil website (DISA website 2012). The Joint Chiefs 6510 series instruction has two Information Assurance titled subject lines, the Marine Corps has one MCO5239.2a, titled *Information Assurance Program*, the Army has one information assurance instruction called a AR 25–2, and DISA maintains one Information Assurance policy for their employees only called DISA 630–230–19 (DISA website 2013).

E. DEPARTMENT OF DEFENSE AND INFORMATION ASSURANCE

Some policies are used by multiple organizations to suit their own special requirements. Information Assurance policy at the DoD 8500 series level documents promulgates the “whats” with respect to the requirements. As lower Tiers, or Echelons, start to generate their own policy, the “whats” start to morph into the “hows” by the time they reach the Tier, or Echelon Three. The list of policy and guidance for the DoD section maintains 53 line items and the Department of the Navy list three line items. The IA strategy section has six line items. The observation to be made from this list and review of the DISA policy and guidance website is the staggering amount of policy and guidance that appears to be a top heavy amount in the DoD, while Echelon Commands One through Three are left to create their own policy and guidance to meet higher level policy and guidance by uniformed personnel who are not necessarily experts or scholars of Information Assurance. A contributing factor to this offset is the high number of civilian IT and IA professionals at the program of record and program sponsor level,

defense contracting sector, and the DoD. In addition, observations of the body of attendance at the National Security Agency IA symposium in Nashville, TN in 2011, made it clear that active duty IT/IA experts are in the minority (NSA IA symposium 2012).

The Information Assurance label that has been well branded for many years appears to be being phased out and replaced with a new title catch phrase called "Cyber Security" by the DoD IT/IA community (NSA IA symposium 2012). Although Cyber Security may be an appropriate term for being connected to the Global Information Grid (GIG), it should not replace the industry accepted definition of Information Assurance that still is used in a mainstream understanding.

1. TYCOM AND UNIT LEVEL

The IA goal for commands should be to chart a path towards compliance in the Submarine Force, through proper preparation and support of their IT staff and not just following the tides of expected reactionary requirements to the last IA violation or TYCOM inquiry. Proper documentation is paramount in preparation.

The various documentation related to the Submarine Local Area Network (SUBLAN) consists of Department of Defense and Navy instructions, Type Commander CYBER-1 publications, Specific Information Security Policies, the Common PC Operating System Environment (COMPOSE) Requirements, user guides as provided by various program management organizations, guidance originated by Commander Tenth Fleet (COMTENTHFLT), and other military support organizations, and a constant barrage of official Naval messages. With the overwhelming amount of documentation made available, not all of it covers the entire spectrum of network security and troubleshooting there is to consider. As networks advance, problems arise that are not always covered with documentation or training and usually end up chasing the ever-expanding SUBLAN network. Submarine networks should not be thought of as utilities; they are the *other* combat system and must be treated as such.

II. END-TO-END SECURITY CONCEPT

A. WHAT IS END-TO-END SECURITY

End-to-end security and the various forms it takes is a phrase that is often used and equally misunderstood. “End-to-end security,” “end-to-end network security,” “end-to-end security-defense-in-depth,” et cetera, are all terms with many meanings. End- to-end can mean data origin to data destination—through the operating system, while in storage, over the wire, over the radio, in routers—where data is never unprotected, from the point where the data originates to the point where it is destined.

Another way to think about end-to-end security, within the context of Information Assurance, is to think of it as “from writer to reader” or “cradle to the grave” protection of data and information. Regardless of how it is phrased, end-to-end security can be tested when it is observed that the protection is effective and protection is never removed anywhere through the communication or operating systems. For the purposes of this thesis, protected data will be considered to be data that maintains confidentiality, authenticity, and availability.

This section focuses on end-to-end security as a summation of the information assurance trade space previously described. The information assurance trade space, discussed in this thesis, is traditional information assurance (confidentiality, integrity/authenticity, availability) and additional integrated information assurance (training, personnel, equipment), which together are capable of providing end-to-end security. Although integrity is a lessor subset of authenticity, non-repudiation, as used in the IA context, is also a subset of authenticity as it is applied to a receipt system such as Public Key Infrastructure (PKI). An application of authenticity is digitally signed (S/MIME) e-mail. Within the integrated IA category of equipment, software security tools should be included as a subset due to Information Systems (IS) equipment’s dependency on software to supplement hardware or act solely independent.

B. WHAT DOES END-TO-END SECURITY PROVIDE

All end systems should attach to a routable LAN/WAN of some form. But not all communication systems that terminate from end user to end user are 100% secure. The corollary is that no end system should put data onto that LAN that has not been protected. End-to-end security must protect data in storage as well as in transit. Using the term “protected” does not mean encrypted—there are no cases where authenticity is not a requirement, so protection should always include digital signatures. If confidentiality is required, then “‘protection” includes encryption too. If the communications system that handles the data is a routable network, then it has the highest chance of becoming secure from end-to-end.

C. WHAT IS NOT PROVIDED WITHOUT END-TO-END SECURITY

Unlike shore based enterprise networks, such as Navy and Marine Corps Intranet (NMCI) or Outside Continental United States (OCONUS) Navy Enterprise Network (ONE-Net) that use Common Access Cards (CACs) to authenticate users, almost all shipboard networks at the General Service (GENSER) classification level and lower do not have a method of digitally signing data from that command or user; nor is there a bulk data encryption process. An entire ship with user logon and password, as the only method of network access, can and does create its own data objects in a shared environment. While this may assure the authenticity of the organization that owns the data, the individual user who created the data is not authenticated in such a fashion as to provide traceability—in short, from actual writer to reader. An example of how data flows through the OSI model is provided in Figure 2.

Due to implementation of this type security, this middle ground continues to challenge networks and their administrators, especially if the physical or network security fails—the data can be compromised.

In 2010, the Navy implemented Computer Tasking Order (CTO) 10–25, as issued by COMNAVNETWARCOM, an attempt to provide an extra measure of security for what was considered removable media CTO 10–25 is specifically intended to utilize

Commercial Off-the-Shelf (COTS) Host Based Security System (HBSS) software and Navy policy to prevent access to any removable media hardware or software such as a USB device. CD/DVD write capability is disabled on each workstation by the system administrator. The misconception by most is that the implemented HBSS is 100% prevention of unauthorized removable media for onboard workstations. HBSS does not control the data itself. In fact, HBSS onboard submarines only detect any USB device once it has been plugged into the host computer. The IT operator must review the logs manually to discover and investigate the USB violation.

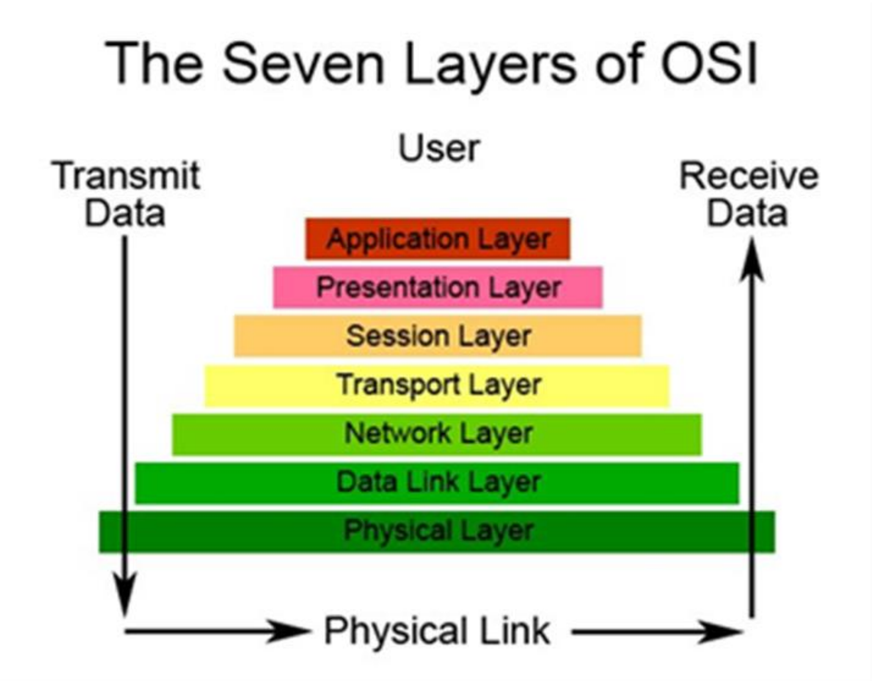

Figure 2. OSI Model

D. THE OSI AND TCP MODEL

Two basic questions should be considered when addressing end-to-end security with respect to the Open Systems Interconnection (OSI) model:

- What layer of the ISO model is security being applied to?
- What is the object that is being protected?

These are two different ways of asking exactly the same question. For example, if the object being protected is a datagram, then the network layer in question is Layer 3. End-to-end network security in reference to the Internet happens at Layers 6 or 7, the presentation and application layers. Lower layer protections are not 100% adequate, because the scope of those layers is less than end-to-end. Inadequate examples include, but not limited to, the Navy Marine Corps Intranet (NMCI) and the Hypertext Transfer Protocol Secure (HTTPS), because there are no protections within the end systems' operating systems.

More prudent examples of end-to-end security within an intranet are signed and encrypted e-mail, Secure Shell (SSH) (SSH is a secure network protocol used for remote secure network services between a server and a client) and Voice Over Internet Protocol (VOIP), which is similar to how the Skype application works.

Figure 3 is provided to compare the OSI model to the TCP/IP model. The OSI model is a reference model and the TCP/IP model is an implementation of the OSI model. The TCP/IP model was derived from the DoD's original Advance Research Projects Agency Network (ARPNET) and adopted by the International Standards Organization (ISO) in the late 1970s as a framework for describing all functions required of an open interconnected network. It is a widely known and accepted reference model in the data communications field and is used here only for comparison purposes (Microsoft 2013).

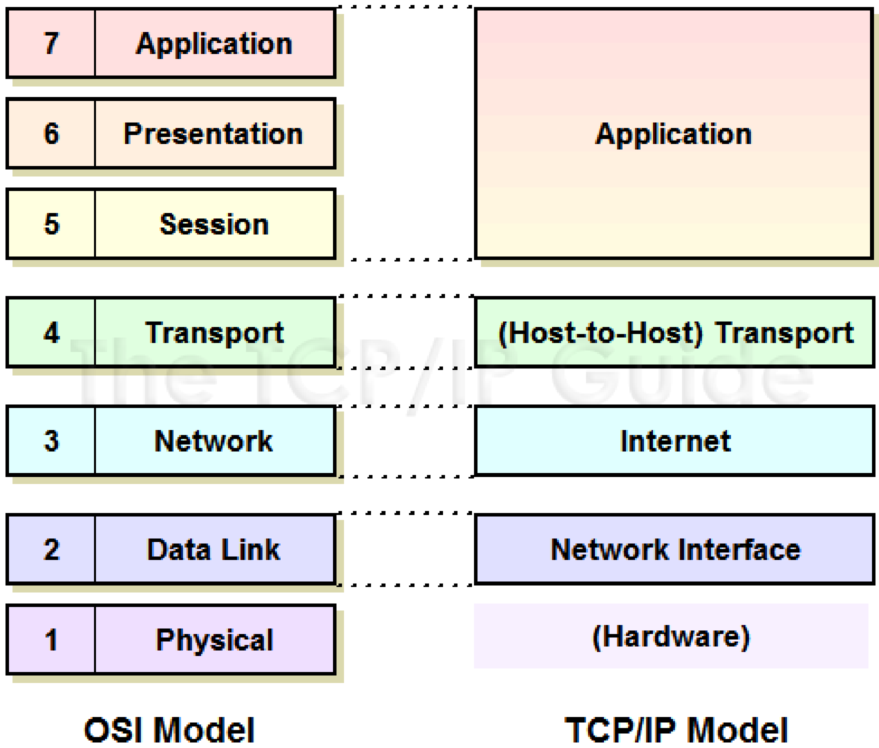

Figure 3. OSI vs TCP Model

The security implication is that security implemented at Layers 6 and 7, the application and presentation layers are embedded in the application, thus are not part of the infrastructure. E-mail signature/encryption is a classic example—these security functions are part of the e-mail user agent implementation. Another example is password protection of a document that is digitally signed or the use of Voice Over Internet Protocol (VOIP).

E. OSI MODEL DESCRIPTION

The following is detailed description of data flow through the OSI model depicted in Figure 2 with respect to end-to-end security concept described in Article II of this research.

Layer 1: this is part of the transport service. For example, radio communications use key generators to encrypt the data. This is a Layer 1 encryption device, which does

nothing more than byte substitution. The object protected is individual bytes (frame and IP datagram headers included).

Layer 2: The functions of Layer 2 are 1) interface to Layer 3 and 2) media access control. This layer can encrypt a frame, or individual bytes of data. It can be argued that this constitutes Layer 2 protection. Either way, the scope of the protection at this layer is single-segment—all of these protections must be reversed in order to recover the contents of the data.

Layer 3: Data protection is typically on network segments at Layer 3 or lower. There are unclassified, secret, and top secret enclaves that connect to routers at this layer. In this case, the object being protected is an IP datagram where the user's data resides.

Within Layer 3 Infrastructure are enclaves nested inside enclaves. This is fine for infrastructure protection but not for content protection. For example, what if an end system such as a computer in the submarine has malware in its OS distribution? The current structural strategy creates a "secure enclave," inside which data is rarely protected. Attempting to achieve data content protection via infrastructure protection has varying degrees of success in preventing an outside attacker from compromising sensitive data. It has a near-zero success rate in minimizing compromise by individuals already inside the enclave; access to the enclave nearly always results in access to all the data in the entire enclave. The insider threat or need-to-know concept becomes real and may become impossible to address at the system level. The term insider threat is basically any accidental or intentional act upon a network by the system administrators or users.

Layer 4 and 5: This is the layer that deals with providing a protected connection via a Secure Socket Layer (SSL) and Transport Layer Security (TLS). These methods are normally transparent to the user and protect the data between users or hosts. Unfortunately, security is stripped away at the TCP socket on the end users computer. A socket is the combination of a host IP address and virtual port number (Dean 2013, 164). This, obviously, does not provide "end-to-end security." But it does provide end-to-end TCP reliability at layer 5 for opening and closing the 3-way handshake so no data gets sent without receiver being ready for it.

Layers 6 and 7: This is the application layer and is the start and finish of data by users. Layers 6 and7 seem to be routinely omitted in the widely used term end-to-end security. The function of Layers 6 and 7 is where application interfaces function. Think of this layer where the user opens a word processing program, for example. End-to-end security measures cannot be solved at any layers lower than Layer 6 and7. The lower layers are all agnostic about applications. For example, a TCP connection is just a connection; it does not "care" about whether the connection supports an Internet transaction, e-mail transport, or other.

F. SUMMARY

End-to-end security is complete data protection from writer to reader as the data travels through the entire OSI and TCP/IP model. Due to advancement in hardware/firmware, the easiest and most popular protection model is within a network's infrastructure. Simple network access via a token or common access card will not provide end-to-end security unless that model is applied and ends at application Layer 7. But, if protection is applied to the data from writer to reader and not just the communications infrastructure alone, then true end-to-end security starts and ends at (application) Layer 7, before data is sent on the network to the end user. Therefore, end-to-end security measures cannot be truly solved at any layers lower than that without addressing the entire OSI/TCP/IP model working together within the IA trade space as a System of Systems.

The development of the TCP and IP parallels the development of the OSI model. IP is connectionless and stateless which means that there's no sense of end-to-end connections. Packets of data can get lost for many reasons, but the connectionless nature of IP means that we have a dynamite ability to transparently add alternate routes and improve system availability.

IT operators and system administrators must understand the concept of end-to-end security so as to put in place necessary measures for a proper end-to-end security model. Lack of understanding of this concept by submarine network program managers

inadvertently causes a lack of acquisition and policy support necessary to keep up with dynamic network security measures. Senior leadership should understand the end-to-end security concept in order to understand the cause and effect on overall ship mission and support functions. They need to know what questions to ask and demand closure from TYCOM via the program managers.

It is recommended further research and trade studies be conducted for end-to-end security solutions onboard submarine networks such as SUBLAN. The use of Public Key Infrastructure (PKI), Common Access Card (CAC), or similar token access card used in conjunction with the proper application will provide end-to-end security at all layers of the OSI and TCP/IP model. This will not only prevent loss of sensitive information via loss of data, but make it easier to mitigate the insider threat.

It is recommended further research be conducted to insert end-to-end security training into the submarine ITS training pipeline. Currently, the only network security training is the necessary material to obtain the Security Plus certification.

III. TECHNOLOGY DRIVEN PRODUCT ARCHITECTURE

A. BACKGROUND

One of the most technologies-driven product architectures in the last 20 years is the Internet. If there is anything which demonstrates the power of a routable network, it is the fact that the fundamental core of the Internet is virtually unchanged since it was first conceived of and then has undergone various changes to how it is seen and used today.

In the early 90s, people used to dial into a friend’s Bulletin Board System (BBS) with a modem. In the early days of computers, this type of connecting to each other was referred to as a point-to-point connection, from a computer with a modem that would direct dial into another modem that connected to a computer on the other end. They were typically 64K baud data rate, which was the typical operational speed of that time period; not incredibly fast, for the most part, but generally reliable. Data was transmitted in a First-in-First-Out (FFO) serial transmission method. This connection typically took place on a leased line or a switched circuit.

But three basic concepts changed everything. These three basic key concepts of packet routing, best effort, and protocol hierarchy are the reason the Internet as “The Internet” and has survived, with its fundamental architecture remaining unchanged.

The first concept was that of *packet routing*. The basic concept of packet routing is where the host, or user workstation, data is specifically routed by an Internet Protocol (IP) address to another specific host or user workstation.

The second concept was an idea, summed up with the phrase “best effort is good enough” which was a huge breakthrough concept. Although all communications systems can be viewed as *best effort* in some way or another, b*est effort* is also a result of significant improvement in bandwidth efficiency that packet switching delivers over circuit-switching.

The third concept was that of a “protocol hierarchy,” that is, a very careful and clear organization to the structure of the data that moves, starting from a user

workstation, across the Internet, to a final destination. The Open Systems Interconnection (OSI) model is the primary model used to describe this concept. An example of the OSI model is shown in Figure 2.

1. Data Packet Routing

The best way to understand the concept of packet routing is to contrast it to a telephone conversation. Telephone systems are basic circuit-switching systems. Before one can make a call, the line must be clear or not busy. In a telephone conversation, data is transmitted voice to voice in a way that is basically continuous. But the designers of the packetized approach chopped up the data into packets; they were not even sure what route these data packets were going to take. But just like a telephone system, before the first chunk of data can pass, there must be an open path across multiple points across the Internet.

2. Best Effort is Good Enough Concept

Reliable packets of data were just launched from the sender to the receiver, (or workstation to workstation), over unreliable components and getting to their destination was just something that was hoped for—the best would have to good enough. If the other end receiving the data was overloaded, it would just drop the packet of data and ask the originator transmitting the data to send it again. Some of the unreliable components in the middle were switches and routers. The designers must have figured, “If we’re going to go with packet routing, all we can do is just send the packets and hope for the best.” The main takeaway here is any route that the packets hop closer to their destination will work and there may be multiple paths to do so. If a route fails, it may be due to congestion and the routers direct the packets to alternate routes. This lack of route determination can be disconcerting at first, but is extremely resilient and an enormous increase in bandwidth efficiency. Although autonomously transparent to the average user, this is the Internet concept as it functions today. But then, to compensate, they created a protocol hierarchy, which is the third piece of genius.

3. Protocol Hierarchy

This concept is where there is a carefully designed set of encapsulated protocols. For a non-engineer or geek, it is difficult to visualize these encapsulated protocols. But the best analogy is that of nested Russian dolls, or "a box within a box within a box" concept. That essentially is the best way to visualize the Internet Protocol, or IP protocol. An IP is this packet of data, also known as a datagram. The end systems do not care what happens in the middle of the protocol hierarchy—it is transparent. The IP does not need to have any functionality other than one-hop forwarding while TCP provides end-to-end integrity which helps prevent lost packets. The tradeoff is TCP is ignorant of how the packets come and go in the first place. Architecturally speaking, both of these can be labeled "modularity." In other words, the payoff to this modularity is one can change something in one layer of the OSI model, as long as interfaces between the layers are intact, and everything else is transparent. Designers can change, hallucinate, and improve applications in end systems entirely transparent to the infrastructure.

The datagram architecture known now came about because of the success of the combination of the three concepts discussed here. This architecture origin provided deliverable content on demand by popular demand.

The Internet was designed to deliver, for the most part, read only content, such as webpage. But the way it has been forced, now, to *accept* content was a function it was never really designed for in the first place. Only after the concept of data owners desiring to restrict access was there the development of forced two-way secure links, login and password requirements, and encryption.

The most significant driver of this concept was Electronic Commerce transactions. The designers or architects of the Internet had no idea what was going to become of these three concepts. If they did, the Internet may not exist the way it does today because—to an expert in security or an average network technician—it would have been evident from the beginning that architecture like this would be vulnerable and has an almost complete lack of End-to-End security, which is entirely different from what goes on below Layer 6.

B. SUMMARY

The takeaway from this chapter is to understand the advances in technology that have changed product architecture. That product was, and still is, the Internet and its ability to function the way it does. Normally a demand will drive a product to be developed for s specific purpose. In the case of the concept of the Internet as now known, advancement technology itself was the main driver behind the Internet architecture. This advancement in technology was felt in the Navy and submarine force and was well taken advantage of for the next step in the Navy and submarine force’s Information Technology ambitions.

IV. IT-21 TO ITS

A. IT-21

1. Background

In the mid-1990s, the Navy's new plan to modernize its Information Technology ambitions was called "Information Technology for the 21st Century" (Vena 1998). Vena focused on competencies of Navy Enlisted IT Personnel for the USN, along with the enlisted manpower training and core competencies required to manage this program upon which the Navy was embarking . The report well identified training requirements and core competencies for enlisted IT specialists. Vena stated, "Will IT training and education be an enabler in reaching the goals of Joint Vision 2010 or will the military repeat the mistakes of organizations that have tried to solve their problems by overemphasizing technology?" (Vena 1998, 2). In other words, the Navy needed to change how it trained those personnel who took care of onboard networks in order to maintain or improve its network-centric ambitions. A junior ITS sailor should be trained and capable of using end-to-end system administration and application security tools. A mid-grade ITS sailor should be trained and capable of properly installing, deploying, and teaching non-IT crew members how to use those tools securely.

This thesis picks up certain sections where Vena's thesis left off by updating particular focus areas such as IT workforce trends, organization, required skills et cetera, while providing new analysis and synthesis particular to the submarine force such as the new IT rate, enlisted and officer IT training and manpower, program and operational level processes, IT interoperability to meet capability, and how Information Assurance as a system of systems should be considered a mission capability for all submarines.

B. INFORMATION TECHNICIAN SUBMARINES

1. Background

Early on, the submarines Fire-control Technicians (FT) were considered the experts, by any early-day definition, in data processing, computers/computing, and

networking, due to their extensive training path system. Occasionally, other submarine rates that assisted the FT division with onboard networking joined in on the collateral duty of managing the ad hoc network onboard. These were also the sailors who were among the first to start experimenting with networking personal computers at home, the extensive use of dial-up connectivity to a local Bulletin Board System, and then with the Internet (and eventually intranets) onboard submarines.

All of the networks on submarines were being installed as ad-hoc Local Area Network (LAN), with only the authority provided by the Commanding Officer (CO) of that submarine. Once a couple of boats put together their first LAN, CO envy would spread like a computer virus—every CO wanted a LAN. There was no consideration for network security, viruses, equipment, or personnel support, and so on. As long as the submarine could take advantage of increased productivity and information sharing on board and with the submarine Immediate Superior In Command (ISIC), everyone up and down the chain of command was satisfied. This was about to change—personal computing equipment, networking technology, and increased workloads placed on the ad-hoc network and the ad-hoc division that supported it forced a course change that was yet to be charted. The one thing that was certain was the need for official training path system to give sailors the first Navy Enlisted Education Code (NEC) for basic, intermediate, and advance networking training.

2. Pandora's Box

The submarine force is experiencing something new that has not been attempted in decades—the creation of a new technical submarine enlisted rate called Information Technician Submarines (ITS). In the early 1990s, personal computing and basic networking found its way into the submarine force. With Commercial Off-the-Shelf (COTS) personal computing and networking equipment becoming more efficient and affordable, along with smart junior sailors taking up computing as a hobby, it was only a matter of time before the afloat submarine force realized the value of networking all the computers on board a submarine for official and unofficial purposes. What was not realized was the Pandora's Box that was about to be opened. In other words, it is a

process that generates many complicated problems as the result of unwise interference in something. At the time, afloat submarines and their shore commands were so fixated on the Internet and Intranets and their ability to bring communications to almost real-time, the proverbial Pandora's Box was not even thought about with respect to information assurance, manning, manpower, training, equipment, et cetera. The question bears asking: "Did technology drive the Submarine Local Area Network (SUBLAN) product or did fleet requirements drive the SUBLAN product?" The SUBLAN network architecture is an Internet Protocol (IP) technology driven product. A basic appreciable description of IP based driven technology is provided in this thesis and a SUBLAN description is provided in Appendix A.

C. SUMMARY

The Navy's IT-21 program was off to a good start with establishing a plan to modernize, standardize, and take advantage of the new networking technology that enabled Command to communicate in a non-traditional fashion with a non-traditional system that was maintained by non-traditional sailors as a collateral duty. IT-21 worked for many years until networking became less of a luxury and more of a requirement. IT-21 program was not update as fast as technology and the demand for connectivity increased. Subsequently, the need for higher trained and dedicated operators, technicians, and officers also increased. Almost two decades later it became apparent that the concept of a new battlespace may exist and a new design to deal with that battlespace and revitalize traditional battlespace warfare was needed.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DESIGN FOR UNDERSEA WARFARE JULY 2011

A. BACKGROUND

Discussing the future of undersea warfare design, J.F. Caldwell and J.M. Richardson and R.P. Breckenridge state: “we will need to fight our virtual ship in the cyber domain as capably as we fight in the undersea domain” (Caldwell, Richardson, and Breckenridge 2011, 4). The question becomes, then, how can the Submarine Force Combatant Commanders better prepare and improve its Information Technician (IT) personnel, equipment, and training to meet increasing submarine warfare requirements worldwide, while employing undersea forces and delivering future undersea warfighting capabilities without unnecessarily sacrificing valuable monetary and manpower resources? Further description of the DUSW is shown in Appendix B.

The answer to this question postulated in this thesis is by a thorough and solid paradigm shift in understanding Information Assurance (IA) as a systems of systems in the submarine force that revolves around a trade space comprised the traditional understanding of IA being confidentiality, integrity, and availability, also integrated with proper interoperability training, personnel, and equipment that meets current and future capability.

B. INFORMATION ASSURANCE GAP IN DUSW

The Design for Undersea Warfare (DUSW) is a current and active plan to impress and build upon a force-wide realignment for developing, supporting, operating, and employing through three primary key focus areas called the “Three Lines of Effort (LOE).” These LOEs are “Ready forces, Effective Employment, and Future Force Capabilities” (Caldwell, Richardson, and Breckenridge 2011, 8).

One of the three LOEs related to IA or Submarine IT are:

- Ready Undersea Forces
  - Establish ITS rating and LAN Division is listed as an initiative with no focus area, instruction, or description
  - Improve IA afloat and ashore is listed as a focus area with no instruction
  - Establish an Information Assurance Workforce (IAWF) program to manage the ITS sailors' qualification progression.
- Effective Employment
- Future Force Capabilities

The intention behind the DUSW Lines of Effort is to provide enough specifics to define the objective clearly, while providing enough flexibility to encourage initiative from the most junior sailor to the commanding officer of the ship. Each LOE maintains a list of specific focus areas, with a corresponding initiative, instruction, and an aggregate description of all three. The line of effort, "Establish ITS rating and LAN Division" is listed with no supporting focus area, instruction, or description. For the first time in many decades, the submarine force created a new enlisted rate called Information Technician Submarines (ITS). In the submarine force's haste to accomplish this task in time for publishing the DUSW, an opportunity for a more appropriate accompanying focus area, instruction, and description or plan was missed. This thesis will examine the personnel and training aspect of the new ITS rating, its shortfalls, and a more appropriate support measure of the LOEs.

The line of effort, "Establish Information Assurance Work Force (IAWF)," is also listed with no supporting focus area, instruction, or description. This LOE initiative should have been omitted because the IAWF was not created by the submarine force. IAWF was actually established by the DoD in 2004 under the DoD reference 8500–01M and currently revised in 2012 as *Information Assurance Workforce Improvement*

Program. Thus, a missed opportunity in creating a Risk Management Framework (RMF) was inadvertently made.

The focus area "Improving IA afloat and ashore," lists initiative as "Information Assurance Portable Electronic Devices Policy," lists the instruction number as "NA" or not applicable, with a description to develop a single portable electronic device (PED) instruction that will support the entire submarine force. This effort was expected to improve commonality between CSP & CSL and improve IA afloat and ashore". It is a conceptual error to assume (more accurately in this case) that a Portable Electronic Device (PED) policy is an appropriate or accurate policy to improve IA afloat and ashore. Proper IA references were and still are available during authoring of DUSW. OPNAV 5339.1C *Navy Information Assurance Program* is the baseline starting point for Naval IA policy.

C. DESIGN FOR UNDERSEA WARFARE UPDATE 2012

In November 2012, the Submarine Force Commanders published an update to the DUSW. The update built upon the force-wide alignment previously generated in July 2011.

Line of Effort, Number 1 is designated "provide ready forces," and this is stated as "Support organizations must develop a more capable shipboard suite, revise our TTP for emerging threats, and protect our own cyber networks." The evidence of improvement to be provided for this line of effort is "IA assessments; deployed mission performance evaluations; Tactical Readiness Exams (TRE) results" (Caldwell, Richardson, and Breckenridge 2012, 5).

Not until the next anticipated update will this evidence of improvement be fully evaluated.

D. SUMMARY

DUSW is a plan to get the submarine force on a new dead reckoning course. Even with some minor shortfalls with DUSW addressing Lines of Effort for IA/IT/LAN

systems, programs, and personnel, a deeper reach to leverage the proper level of experts already embedded in the submarine force will ensure the DUSW spirit of intent behind those LOEs.

VI. INFORMATION ASSURANCE PHYSICAL, FUNCTIONAL, AND BEHAVIORIAL BOUNDARIES

A. BACKGROUND

Information Assurance (IA) is not without boundaries. Through the study of Systems Architecture and reviewing IA holistically as a system of systems, the topic of “information assurance boundaries” relates directly to the Defense in Depth (DiD) Strategy layers.

The DiD, a layered approach towards people, technology, and operations, has many iterations. For example, Cisco’s DiD with respect to a “unified Contact Center Enterprise (CCE) solution” (Cisco Inc. 2009) functionally correlates to IA boundaries.

When it comes to physical, functional, and behavioral IA boundaries, the physical boundary is the closest thing that directly correlates to the physical boundary described in the Defense in Depth Strategy. Knowledge of the relationship between these three boundaries in the traditional Defense in Depth Strategy layers originates from the author’s personal observations and synthesis for many years as an Information Assurance manager, communications manager, and security manager for seven submarines and multiple submarine squadrons. For the purpose of this discussion, the physical, functional, and behavioral boundaries discussed in this context will correlate to the individual layers. Figure 4 depicts the author’s conceptional IA boundaries’ relationship model to a DiD model.

- For example, the physical security layer is directly related to this physical IA boundary.
- The functional boundary correlates to the host security, internal network, and perimeter security Defense in Depth layers.
- The behavioral boundary correlates to the data security layer that deals with application and data.

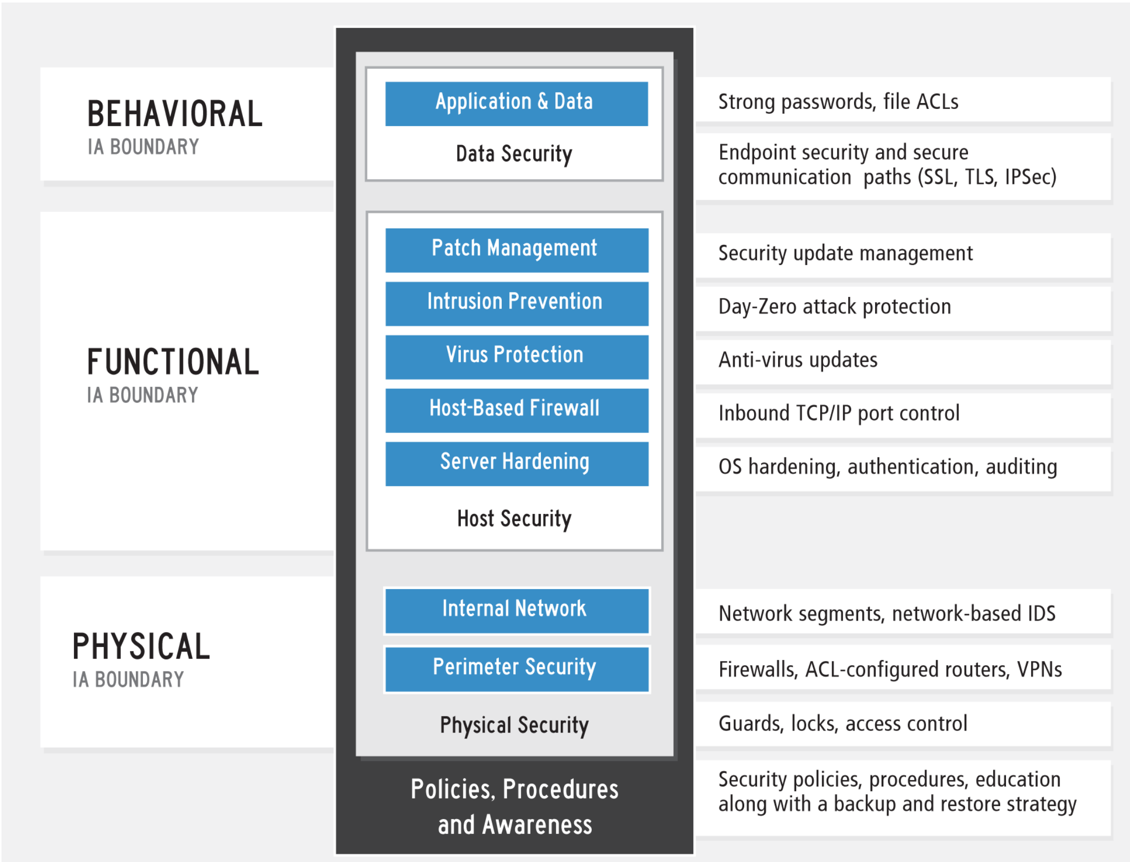

Figure 4. IA Boundary vs. Defense in Depth

To compare this to something familiar in a submarine context, information assurance boundaries can be viewed similar to the submarine safety (SUBSAFE) program, which also contains a multilayered Quality Assurance (QA) process. Understanding these boundaries could also help identify with and understand the End-to-End Security concept. Due to the specific nature of the SUBSAFE program, a detailed description of the SUBSAFE program cannot be covered in this thesis.

For someone involved in the submarine community, it is possible to observe that for the last 25 years, the use of computer systems in the submarine forward compartment (such as Fire Control, Sonar, Navigation Center, Radio, and Missile Control Center) has changed. Whereas in the past, the computer systems were used as tools by trained and experienced sailors to assist in making critical decisions, it is often the case now that

sailors are simply concurring with the decisions made by the computers, as the computers are the sources of information, and the sailors are lacking in the training and experience they once had.

In submarine systems, the old architecture has been dramatically changed with the inclusion and increase of Commercial Off-the-Shelf equipment (COTS), in attempt to make our sailors “smarter” with the data that is given to them. In some areas operators and technicians have done that well with the extra equipment. But in other aspects we have not done well. The systems architecture of those systems has changed in attempt to improve how sailors operate and *fight the ship*. Ill planned operational requirements for new technology have changed and violated the Physical, Functional, and Behavioral IA boundaries of our systems. Older systems on submarines may not be IA compliant, with respect to current DoD IA compliance regulations or as compared to newer hardware and software builds. In this case, the best apparent mitigation is for the local submarine squadron to promulgate guidance for their afloat units for marking, handling, and safeguarding classified data processing systems.

B. PHYSICAL IA BOUNDARY

The physical IA boundary, closely related to IA system security (availability and integrity) can be considered the same as Layer One of the Defense-in-Depth model, being the physical controls preventing access to IT equipment that would further allow someone access to any electronic information system. The typical example given is a secure building with multilayer physical access controls in place such as a sensitive server data farm located in the most inner room with a locked door and alarm system which is also secured by the outer door to the building with a locked door and alarm system. Access to that sensitive server or data farm would also be limited to a minimum number of personnel. Addressing information security (authenticity and confidentiality), a common access card is a good example of the use of this boundary. Without the card, you have no access.

Physical security for submarine is like any typical naval ship. It is typically moored in a secure Naval installation, followed by a physical barrier system of some type before reaching another personnel access control barrier where sailors must verify access for any personnel entering the submarine.

Once below deck, the physical IA boundaries can be somewhat nontraditional. Due to the physical architecture of various submarine platforms, it is not always practical to locate sensitive information systems in a fashion that allows the equipment to be physically locked in a secure space. But with respect to the server racks, or other equipment, they can have physical access controls in place. For example, on Trident class submarines, a Submarine Local Area Network (SUBLAN) server is installed in a space called the Data Processing Room due to the classification of the server and convenience (following a modernization period for that class of ship). Otherwise, none of the unclassified Information Systems equipment, with the exception of a classified server, is designed to be locked. The Los Angeles class submarine platform is no different in comparison to the Trident class. The newer Virginia class submarine took into account the need to isolate and lock classified servers and designed that requirement into the original building plans.

C. FUNCTIONAL IA BOUNDARY

The functional IA boundary correlates to the host security, internal network, and perimeter security layers. Within the host security section of a typical Defense in Depth model, there is

- patch management, also known as security update management,
- intrusion prevention, also known as zero day attack protection,
- virus protection (also known as antivirus updates) host-based firewall (also known as inbound TCP/IP port protocol)
- server hardening (also known as operating system hardening)
- authentication, and
- auditing.

This boundary should be defined and viewed as any process within a system or subsystem that can or does exchange data with another system or subsystem between Layers 2 and 6 of the Defense-in-Depth model. In other words, if one Information System can or does exchange data with another Information System by design or not by design, then it will pass through an Information Assurance Functional Boundary.

The purpose of this model as described is to “provide a conceptual and functional framework” that aids in the concept of IA boundaries as they relate to a specific layer the DiD model. Additionally, this reference model is not intended to be “an implementation specification” and therefore does not exist in a real-world example. Instead, it is meant to visually depict the author’s three IA boundaries in relation to a typical DiD model.

D. BEHAVIORAL IA BOUNDARY

This is one boundary that is the most difficult to identify and control. The behavioral boundary will correlate to the data security and application layer of the Defense-in-Depth model. This boundary has two identifiable areas of concern: applications and human interaction. Both are the first and last information security checkpoints.

Applications, whether compared to the Defense-in-Depth model or the OSI model, may vary in IA controls or in the application’s own security vulnerabilities. Such application vulnerabilities include but are not limited to invalidated inputs, broken access controls, broken authentication and session, management, cross site scripting flaws, buffer overflows, injection flaws, improper error handling, insecure storage, denial of service, and insecure configuration management, and so on. Keeping vulnerabilities identified and patched is a daunting task. In some cases, it is not practical or not possible to fully fix some applications’ vulnerabilities due to the possibility of destroying the application’s availably to its designed functionality. For example, Microsoft Office 2010 is the most integrated MSOffice package ever created. But, because of a wide breath of integrated interoperability, MSOffice has numerous security exploits contained within it.

The human IA boundary is the most difficult to control, regardless of the status of the physical and functional IA boundaries. Human interactions at the application layer can be similar from one person to the next, but a user's reasoning for deciding to do the wrong thing with respect to violating IA controls or Information Security policy can vary greatly as much as the many creative ways to commit the violation. The user in this case is a user who is cleared for classified information, but this kind of user also has, in some cases, the ability to manipulate or even remove that information from the system or network. To put it simply, just because people can commit a security violation via an application on an information system does not mean it will purposefully happen. The significant observation to be made is that the action of the user, not the reaction of the application of that classified system or network may be the source of the violation and not the software.

E. IA BOUNDRIES ONBOARD

The issue at hand is not necessarily with new systems installed on submarines, such as the Submarine Warfare Federal Tactical System (SWFTS), where the IA boundaries are significantly improved, or with the newer Virginia class platforms, where most of the systems have IA concepts designed into the architecture. The focus here is on older systems, such as the Block 1C Fire Control system, Submarine Tactical Display Auxiliary (STDA) system or the typical BYG-1 Fire Control system. These systems are not IA compliant with current IA policies due to their age; when these systems were designed or installed, IA was not considered.

These systems have stood mostly alone for over a decade with a level of interoperability that could be expected for that time. Due to the sensitivity of classified material controls, advances in technology, attempts to make up for shortfalls in long term degradation of navigation, and combat system management, and lack of advanced navigation and voyage planning skills, additional standalone or peripheral systems continue to be installed on submarines to interface with older systems, without any consideration for IA compliance or concept of End-to-End security practices. The intent of these additional systems was to improve capability. Instead, these additional peripheral

systems changed the overall system of systems architecture, thus breaking down the aforementioned IA boundaries, resulting in overall system performance and false sense of reliability, specifically with the submarine combat systems.

Further research is recommended both on this cause and effect of new Information Systems as disruptive technology to older Information systems on board ships and submarines and if ability to safely operate, navigate, and fight the ship has improved with the addition of these new systems. Further research is also recommended to capture reliability data to provide sufficient context to provide an effective standard of evaluation of in-use combat system software and hardware build.

The Fleet is currently challenged in their ability to understand how their combat systems are performing. How much effort should be required to maintain a system performing to design specifications? What amount of sluggishness, or other system problems, is indicative that action needs to be taken?

F. SUMMARY

The concept of IA boundaries as it relates to the DiD model and OSI model is relatively new suggestion. With a basic understanding of those models and IA, a direct correlation can be observed. With a basic understanding of IA and the operation of those systems that this research addresses, the concept of IA boundaries can be understood by operators, technicians, PMs, and leadership. IT operators and technicians are among the highest priority to understand this concept and manage all of the IA requirements management. But it will require new personnel, training, and leadership: a new human capital strategy. How will the submarine force build these enlisted ranks with the proper Navy Enlisted Education Code (NEC) and training while managing the overall manpower and resources for the submarine missions that rely on complex networks?

THIS PAGE INTENTIONALLY LEFT BLANK

VII. HUMAN CAPITAL STRATEGY

A. MANNING

"The establishment of the ITS rating will provide the Submarine Force with an infrastructure of information assurance and network professionals who will be fully equipped to resolve future issues and implement new technologies on board our submarines" (Public Affairs, United States Navy 2010). But the new rate has not gone as well as planned. This is the first time the submarine force has created a new enlisted technical designator, or rate, of this kind. Unlike a civilian corporation, the submarine force cannot hire off the streets to fill a need at the E5/E6 level, so they have to find those Sailors who are ready to shift over from their previous technical rate and get them into these billets, while at the same time populate the accession side for future stability. Therefore, a new rate, was required to meet the demand of the submarine networks.

Submarine ITS manning projections continue to show improvement as the submarine force is manned with the earliest A-school graduations reporting in spring 2013. As inventory grows, commanding officers are encouraged to fill their ITS shortfalls from within their crew by submitting an updated ITS division stabilization message, as described below, to Navy Personnel Command Code 403 (PERS-403). PERS-403 will assign these selected Sailors to vacant ITS billets and backfill their respective divisions appropriately. The bottom line on this issue is that the submarine force is building the ITS community from both accessions and divisional cross-decks sailors on board; it does not come without challenges.

B. ITS NEC CONVERSION

The difference between direct and lateral conversion is that direct conversion does not require a formal school as part of the training path, whereas a lateral conversion is via a formal school. When the ITS rate was started, Commander Naval Cyber Forces (COMNAVCYBERFOR) mandated that all IT or ITS rated sailors who hold Navy Education Code (NEC) 2735 and do not hold NECs 2779, 2780, or 2781, are required to

do a direct conversion to their NEC through Delta training, described in several Naval Administration (NAVADMIN) messages released in 2011. On Dec 31, 2012 all 2735 (older) NECs were being phased out and converted to NEC 0000 and those affected sailors could be limited in permanent Change of Station (PCS) assignments, Selective Reenlistment Bonus (SRB) eligibility, and they could receive unfavorable Perform to Serve (PTS) results. Sailors with Naval Education Codes (NEC) 2779, 2780, or 2781 (older LAN NECs) have the option to directly convert their NEC, but are not required to do so; however, these sailors may also suffer the same impacts as the mandatory direct converted sailors and are therefore highly encouraged to convert their NEC directly as well. Some of the sailors who hold these older NECs originate from the Journeyman Network Core (JNET-Core)-NEC 2735, Network Security Vulnerability Technician (NSVT) NEC 2780, Advance Network Analysis-NEC 2781, and Information Assurance Manager-NEC 2779 schools. To track the progress throughout the fleet, a report is sent by Navy Cyber Forces Command to all the Type Commanders (TYCOMs) each month, showing the percent completion rates for each TYCOM; Commander Submarine Pacific COMSUBPAC AOR is currently about 80% or better complete with the 2791 NEC requirements. By January 2013, Commander Submarine Atlantic (COMSUBLANT) maintains administrative control of the conversion, stop tracking NEC conversion due to the significant progress made. But, as of February 2013, “Current ITS inventory is approximately 50% of the force requirement” (COMSUBLANT 2013).

1. Training

One of the requirements to complete the 2791 NEC direct conversion is to have Security Plus certification and NEC 2735. This is the most difficult requirement to complete because the sailor either has to study and schedule his own exam or wait for the local submarine squadron to contract an outside training and testing organization. NEC 2790 requires a self-taught IT differences training called “Skills Port” and A-Plus certification.

To help increase the completion rate, one week boot camp style training sessions are being utilized in order to complete the Security Plus certification component of the

direct conversion. The remaining requirements can be completed using Skills Port training, which has been delivered to all submarines via a Skill Soft CD and is also available online. Another method to complete security plus training via standalone software called Carnegie Mellon Virtual Training Environment (VTE) provided by TYCOM.

It is difficult for sailors to complete their courses, due to ships' Operational Tempo (OPTEMPO) and daily workload. Additionally, the biggest challenge for sailors to complete these courses is the limited availability and access to computers on board. There are approximately 6 to 10 public unclassified workstations available for the entire crew onboard submarines. These workstations are typically shared with divisions for work purposes. Submarine Information Technicians have to compete for computer usage and are constantly getting bumped off for higher priority usage of those computers. The training products on board are self-paced and are for self-study and require time and a space for the laptop for the sailors to be able to complete them. Sailors cannot ask questions if they do not understand something, so it is strictly one-way training. The courses are also bandwidth intensive and do not function well using limited peer connectivity and certainly are not available underway. Despite each ship being given training on DVD to overcome the bandwidth problem, submarines are not the best learning environment for Computer Based Training (CBT), as there are limited space and computer resources.

With the constant workload associated management of the networks and Preventive Maintenance System (PMS), it may take several more months for people to complete the courses on board than would be the case if these courses were taken ashore. While information is available for the sailor to complete it, it is sometimes difficult to be technically ready to take the test for certification. To assist sailors in passing the certification exams, "boot camp" style week long courses are arranged by local submarine squadrons. These boot camps take sailors off the boat and immerse them into the material for one week. The key to success is not only focused time away from the workplace and the ship, but also the night study sailors must perform to ensure they

understand the material. Sailors who take the exam immediately after the boot camp course tend to pass the first time, as opposed to the sailor who waits too long after the boot camp course to take the exam or tries to self-study for weeks or months. The Achilles' heel to these boot camp courses is lack of centralized coordination and scheduling. It is left up to the submarines and submarine squadrons to find reliable and qualified vendors to provide the training and certification exams. This is a very inefficient way to train and certify new submarine rate that is in charge of a virtual combat communications system. The submarine force's training and readiness department at the TYCOM level is a much more efficient vehicle and is better suited to coordinate onboard training for the submarine Information Technician.

Currently, there is no way for a ship's Executive Officer of a submarine to schedule his Information Technician to go to school for Security Plus training in advance of approximately 30 days. If the TYCOM Training Readiness Department coordinated all aspects of the boot camp schools, afloat commands could actually plan ahead for sailors to attend training to complete their Security Plus Certification.

The current ITS NEC breakout for SSBN submarines, for example, is two 2791 (E4-E7) and two 2790 (E1-E5) ITS school graduates), so the senior enlisted pay grades still have to come from the boat. PERS-403 continues to work closely with the enlisted community manager (ECM) as this rating is established. The A-school pipeline is expected to start producing graduates in 2013. Until that time, there is a lack of distributable ITS inventory to fully staff every ITS division. It will be necessary for commands to continue to backfill their divisions from onboard personnel. Replacements will be identified form a source rating of onboard crewmembers.

C. ITS MANPOWER

In order to track and report this process, PERS-403 has been (for almost two years) directing afloat commands to submit LAN stabilization messages (Figure 5) whereby PERS-403 would review with the appropriate detailers and respond by message (Figure 6) with concurrence or non-concurrence for sailors to convert to the new ITS rate.

In order to grant concurrence, the sailor's detailer and community manager must be able to support losing that sailor from their current manpower inventory. A common and critical error made by the afloat Command is reassigning a sailor to the ships IT division and allowing that sailor to work for months, sometimes up to a year and a half before submitting a direct rate conversion package. The request is sometimes disapproved due to the sailor's parent rate being undermanned. The parent rate is the sailors first enlisted rate before converting to a new designator. The result is a sailor who has not functioned in his original contracted rate for an extended period of time is still required to take advancement exams from his parent rate for which he is no longer proficient. Additionally, that sailor sometimes gets reassigned back to his old rate due to not being able to convert to the new ITS rate. Prior to deployment, a submarine may transmit a LAN division manning message (Figure 6) showing the complete makeup of the division.

The task of NEC managing has been placed on the afloat Command. The burden should reside between the TYCOM and local submarine squadron. The submarine squadron was omitted from the process of screening IT direct rate conversion packages. This omission resulted in many conversion requests being denied that should have been approved, and many that were approved that should have been denied. In other words, quality assurance checks at the squadron level may have improved the selection process. For a more accurate manning picture, the ship would send a message similar to Figure 7

"While previous practice was to set Navy Manning Plan (NMP) (distributable inventory) equal to Billets Authorized (BA) (funded requirement) during creation of the ITS rating, at the most recent NMP working group, the decision was made to set NMP to actual projected inventory to correctly shape expectations force-wide" (COMSUBLANT 2013). This decision was in response to continuous unfavorable feedback from afloat commanding officers to the submarine administrative officer corps about not being properly manned with ITS sailors. Subsequently, the NMP was lowered in attempt to give the perception that the ships are or will be officially manned by meeting the NEC requirement held on board, regardless of the sailor's billet. "Over accession in two other ratings (FT and ET-NAV) produced distributable inventory that allows setting NMP

higher than BA (+1 or +2) for each rate for each crew. These sailors in excess of requirements should provide sufficient capacity to continue manning LAN divisions until the ITS pipeline steady state capacity can produce adequate distributable inventory (NMP at least 85% of BA)" (COMSUBLANT 2013). Other than the analysis previously described, the error made here is the impression of no longer requiring higher throughput for the new ITSs A-school due to an unanalyzed assumption that the submarines can, will or should be managing the ITS manning, manpower, and NEC conversions properly; it simply is not their duty to do so.

R 251200Z SEP 13
FM USS AT SEA
TO COMNAVPERSCOM MILLINGTON TN
INFO COMSUBPAC PEARL HARBOR HI
COMSUBGRU NINE
COMSUBRON SEVENTEEN
USS AT SEA
BT
UNCLAS //N02300//
PASS TO OFFICE CODES:
COMNAVPERSCOM MILLINGTON TN/PERS-403/
MSGID/GENADMIN,USMTF,2008/USS AT SEA/002/SEP//
SUBJ/LAN STABILIZATION UPDATE//
GENTEXT/REMARKS/1. THE FOLLOWING PERSONNEL ARE DESIGNATED AS LAN DIVISION MEMBERS ONBOARD USS AT SEA (SSBN-733)(BLUE):

NAME	RATE	SSN	NEC	PRD
SAILOR, JOE	MMFA/E-2	2441	4231	1608

2. SHIP HAS MOVED MMFR SAILOR FROM AUXILIARY DIVISION TO LAN DIVISION AT MEMBERS REQUEST. MEMBER HAS PREVIOUS INFORMATION TECHNOLOGY EXPERIENCE AND IS HIGHLY MOTIVATED TO IMPROVE LAN DIVISION PERFORMANCE ONBOARD USS AT SEA.//
BT
#0001
NNNN

Figure 5. Sample LAN Stabilization Message from the Submarine

R 261200Z SEP 13
FM COMNAVPERSCOM MILLINGTON TN//PERS403//
TO USS AT SEA
INFO COMSUBPAC PEARL HARBOR HI
COMSUBGRU NINE
COMSUBRON SEVENTEEN
USS AT SEA
BT
UNCLAS //N02300//
MSGID/GENADMIN/COMNAVPERSCOM MILLINGTON TN/-OCT//
SUBJ/LAN STABILIZATION RESPONSE//
REF/A/MSGID:GENADMIN/USS AT SEA/ R 020807Z SEP2012//
AMPN/REF A IS LAN STABILIZATION//
GENTEXT/REMARKS/1. REF A WAS RECEIVED AND REVIEWED.
ALL PERSONNEL ARE VERIFIED AS MEMBERS OF LAN DIVISION.
2. PERS403 SENDS.//
BT
#0002
NNNN

Figure 6. Sample LAN Stabilization Message Response from COMNAVPERSCOM

R 271200Z SEP 13
FM USS MORE AT SEA
TO COMNAVPERSCOM MILLINGTON TN
COMSUBPAC PEARL HARBOR HI
INFO COMSUBRON NINETEEN
NSSC BANGOR WA
BT
UNCLAS //N02300//
MSGID/GENADMIN/USS MORE AT SEA/003/OCT//
SUBJ/ LAN MANNING FOR USS MORE AT SEA (53886)//
GENTEXT/REMARKS/1. THE FOLLOWING INFORMATION IS PROVIDED
REGARDING LANN MANNING FOR USS MORE AT SEA FOR UIC:53886

FULL NAME	RATE/PAYGRADE	LAN NECS
GAETES, BILL	ITSC/E7	2781/2791
JOBS, STEVE	ITS2/E5	NONE
ZUKERBERG, MARK	ET2/E5 (COMMS)	14RO
PAGE, LARRY	ETSN (NAV)	NONE//

BT
#0003
NNNN

Figure 7. Complete LAN Manning Message

D. ADDITIONAL ITS CONVERSION OPPORTUNITIES

In early February 2013, COMSUBLANT sent a message to the submarine force stating, “A recent increase in capacity at the A and C-schools creates the opportunities to open up lateral conversion opportunities for submarine qualified sailors” (COMSUBLANT 2013). What this message means is that the submarine force previously denied lateral conversions to the ITS rating for sailors without an IT background due to insufficient student quotas for the necessary training to level the playing field for converted ITS sailors. The reason there is an increase in capacity in the A-school is due to lowering the NMP as stated above. “Submarine warfare qualified sailors who do not have the required 2790 or 2791 NEC may apply for lateral conversion and, upon approval, be written PCS orders to A-school and C-school to obtain the requisite NECs” (Update on the status of the ITS community and conversion

opportunities” 2013). In other words, a sailor who wants to be an ITS does not have to do any of the onboard training but can wait to be converted via formal training.

The personnel who are responsible for Command and Control on many afloat units are not sensitive to or completely aware of the IA requirements management, PMS, daily operation, reporting requirements, security requirements, and the process required to train and convert old outdated IT NECs to a current more relevant 2791 NEC.

In this confusing roadmap, the Submarine Force has allowed three different paths for sailors desiring to convert to the ITS rating. First, a submarine qualified sailor who does not have the required 2790 or 2791 NEC may apply for lateral conversion and, upon approval, will be ordered to official IT school. Second, submarine warfare qualified sailors who obtain the 2790 NEC utilizing onboard training may be ordered to school to obtain the 2791 NEC and subsequently converted to the ITS and returned to sea duty. Third, sailors may obtain the 2791 NEC by completing onboard and civilian training and certifications or equivalent to that received in the official IT school. Upon completion of that training, sailors must submit a request to be awarded the 2791 NEC. Each of these methods, aggregated together, do not come without consequences. In conversion request, commanding officers should be very clear on when they would be willing to allow the sailor to separate from a command with the understanding that any replacement personnel may take 6 to 9 months to fill that billet. Also, if the sailor is selected for conversion and the command is unable to support temporarily losing the sailor during his seat tour to attend official IT school, the sailor in question should be able to attend that school upon normal detachment from sea to shore duty.

E. RESOURCES VS. TRAINING

Some properly trained non-Navy IT professionals might find a submarine network very rudimentary. Training and equipment are fundamental assets to the Submarine Local Area Network. Without either, the SUBLAN would come to a standstill. On-the-job training has become the primary method for sailors to learn how to maintain the SUBLAN. Most of the problems seen in the fleet are not replicated in the training lab. Navy Enlisted Classification (NEC) codes give a baseline, but not enough to meet the demands of a SUBLAN Administrator. Currently, Journeyman Network (JNET),

Network Systems Vulnerability Technician (NSVT) and Advanced Network Analyst (ANA) schools are all approximately six weeks long and come with NECs, 2735, 2780 and 2781, respectively. Some components of the SUBLAN, such as NIAPS, Global Command and Control System-Maritime (GCCS-M) and Non Tactical Data Processing Subsystem (NTDPS) are not covered by formal training. Some of the SUBLAN Onboard administrators indicate that six weeks is not enough time to learn the many aspects of the SUBLAN. Hardware and software care are covered by the Preventive Maintenance System (PMS). Following the PMS guidance and SUBLAN set up configuration, and accomplished per the PMS, ensures that virus and firewall protection are in place. Switches and servers are rebooted from time to time as needed to maintain sustainability of the network. A new ITSs A-School was brought on line in 2013. Further research is recommended for the new ITSs A-school effectiveness to meet fleet needs.

F. SUMMARY

When reviewing this problem, it is possible to observe that there are two significant, but unofficial, types of submarine Information Technicians. The first type is the Information Technician who has been fully converted with the 2791 NEC, filling the Information Technician billet in accordance with the LAN stabilization message, but is being leveraged to work outside the LAN division supporting that sailor's division and rate; the LAN is treated as a secondary and collateral duty.

The second type of Information Technician is that sailor who is working in the Information Technician division either as a part-time collateral duty or full-time, but who is not a fully converted information technician. This is clearly poor personnel management, due to observations previously mentioned above and misplaced contributions by sailors being tooled and used for one job, yet being tested and advanced in rate in which they have not functioned for an extended period of time. The author of this thesis can only observe this is a lack of sensitivity to a core group of sailors forced to take care of the ship's network; what once was considered a collateral duty has become a full-time job. However, this task is still *treated* as though it is a collateral duty. Needs, requirements, and functions must synchronize.

VIII. IA REQUIREMENTS MANAGEMENT

A. BACKGROUND

The submarine force lacks the ability to comprehensively manage Information Assurance (IA) and associated security requirements promulgated by operational and administrative authorities through TYCOMS, ISICS and to/from subordinate afloat commands. Current IA requirements management solutions and related training are not available. Historically, IA related policies, directives, instructions and related guidance documents reflect what is required; however, they do not provide sufficient detail as to how to satisfy and manage requirements relevant at the tactical level.

Afloat commands are required to maintain and manage IA and related documents specific to the systems installed aboard their respective commands, primarily the System Security Authorization Agreement (SSAA) and Authority to Operate (ATOs). The SSAAs contain system specific technical, administrative and physical IA requirements and must be maintained, reflecting system changes specific to the afloat command. Systems ATOs are typically issued for a period of three years and afloat commands need to manage these documents to ensure they remain current and valid. Afloat commands are also required to maintain and manage IA and related compliance requirements to include Information Assurance Vulnerability Alerts (IAVA), Federal Information Security Management Act (FISMA) and Communications Tasking Orders (CTO).

The DoD 8570.01-M Directive is the Information Assurance Workforce Improvement Program. The 8570.01-M directs that all Information Assurance Workforce personnel must become compliant with the mandated IT and Security certification standards; this also includes the enlisted ITS Sailors. There are various levels of compliance based on the position of the personnel in the IT/IA workforce. The most common certifications included A+, Network+, Security+, Certified Ethical Hacking (CEH) and Certified Information Systems Security Professional (CISSP) (Grimes 2012, 91).

Although compliance and management of IA requirements at afloat/tactical command levels are generally administrative in nature, the lack of effective management of either could indirectly affect an elevated threat to data, systems, networks, and makes it necessary for a significant numbers of man hours to be used to address related issues in the tactical submarine environment. There continues to be no one source for any submarine afloat command to manage IA requirements. In addition, online accounts designed for the IT workforce appear to grow over time.

There are a myriad of required on line accounts for the ship's Information Assurance Manager (IAM) and System Administrator (SA), to include but not limited to:

- Online Compliance Reporting system (OCRS) https://www.iava.navy.mil
- Naval Networks https://navalnetworks.spawar.navy.mil
- COMPACFLT SEAT1 https://cpf2.nmci.nacy.mil/rita/desktopdefault.aspx
- Navy Information Security https://infosec.navy.mil and https://infosec.navy.smil.mil
- Total Workforce Management Services (TWIMS) https://twms.nmci.navy.mil
- Skill Port Navy https://navyiacertprep.skillport.com
- VRAM 2.0 https://vram.spawar.navy.mil
- Navy IA Portal VRAM 1.0 https://www.iaportal.fnmoc.navy.smil.mil
- Sailor 2.1 https://sailor.nmci.navy.mil and https://sailor.spawar.navy.smil.mil

The source for this sample of required accounts is derived from various promulgations by TYCOM and 10 th Fleet.

B. INFORMATION ASSURANCE IN SUBMARINES AND THE OFFICER CORPS

Both current junior enlisted and junior officer ranks are in need of assistance that they need understandable policy that governs IT/IA manning and equipment. IA awareness is increasing, but not at the right operational or administrative level. There remains a significant level of knowledge gap between Echelon 2 and 3 in the overall understanding, implementation, and management of IA. This level of knowledge gap is

most profound at the Command and Control executive level. The Immediate Superior in Command (ISIC) is the afloat unit's squadron major commander. At no fault of their own, most Major Commanders and their senior deputies still do not fully understand IT or IA requirements management. Unfortunately, current executive level senior submarine officers do not view IT/IA knowledge as a core competency, or as an important inspection-worthy attribute; they simply do not have the time to understand how IA as a system affects currently installed systems.

1. Generation Gap

Until the generation gap between senior and junior afloat officers is closed or there is a significant setback, such as breach of information security, and/or direction from higher authority, this lack of sensitivity is not expected to show improvement. The junior officers in the wardroom are a product of society where technology, networking, and information system security have advanced together. It may take another five to ten years for current junior officer department heads, who grew up on technology and are more sensitive and receptive to the importance of information systems, to be promoted the executive officer and commanding officer's level and effect change. In the meantime, current senior leadership continues to view and utilize IT/IA function as a collateral duty. The enlisted technical experts are more receptive to the importance of information systems as a valuable core competency for submariners.

The current submarine communications division officer, normally a first tour Ensign or Lieutenant Junior Grade Officer, and the ship's navigation officer, is charged with and responsible for oversight of IT/IA/LAN onboard the submarine itself. Submarine squadron communications officers who are previously enlisted (8 years or longer) Limited Duty Officers (LDO) are the best equipped to take on this new burden. Their experience, wisdom, and technical ability allow them to adapt to dynamic changes in their profession. Senior leadership, as mentioned above, must support the communication LDO leadership and what they bring into a complex and new systems of systems for the submarine force. Submarine squadron communications officers are

adapting to this new IT/IA/LAN workload—but it is not fast enough and they do not have enough support.

In fairness, senior leadership, to include second tour department heads on board the submarine are simply overloaded with day-to-day functions and/or simply do not have the resources to expend on a new (now full time) technical rate. The current IT chain of command on a typical submarine starts with the junior technician, senior technician, Information Assurance Officer (IAO), Information Assurance Manager (IAM), XO, and CO. Due to manpower shortfalls and onboard manning mismanagement, most submarines, the technicians and the IAM is the same person. The submarines' navigation officer is the IAM. Relief must be sought to shore up and strengthen the IA boundaries, so as to maintain and "fight the virtual ship." Current system designs, manning, policy, and a lack of interoperability burdens the sailor and requires the onboard command and control element to compensate as best as possible.

C. FUTURE IT OFFICER

Over the last few years, IA and the critical importance of networking have been recognized by every level in the chain of command. Submarine Communications Limited Duty Officers (Sub LDOs) with the designation 6290 are expected to be experts in networking and IA in addition to the more traditional C4I areas. 6290 LDOs are finding themselves at a significant disadvantage in that almost all of them arrive at their first billet with no networking and IA training and potentially dated C4I knowledge. Submarine Communications LDOs as IA workforce personnel are required to attain Information Assurance Workforce (IAWF) Level 1 certification (Grimes, 2012, 25). In order to save money, the submarine force does not route new or current 6290 LDOs to any official training to meet DoD 8570.01-M requirements. Currently, those LDOs are expected to obtain Level 1training and certification via their own professional or personal resources. In order to fully support their assigned command and facilitate completion of IAWF level 1, all 6290 LDOs should attend a networking school and IA Manager school prior to reporting to their first officer billet. The Information Dominance Warfare Officer (IDWO) community maintains a training path system for their Information Professionals

(IP) 1820 officers. The submarine force continues to lag behind the forward leaning 10th Fleet and IP community by not properly training and integrating the 6290 LDOs into the IDWO IP 1820 community.

Current 6290 LDOs versus future 6290 does not match up to fleet support. Current 6290 LDOs are prior enlisted submarine radio Chief Petty Officers or First Class Petty Officers and are commissioned between eight and 15 years of service. Most of the 6290 LDOs do not have an IT background, unless they learned it on their own, attended official training, or on the rare occasion, were commissioned from an enlisted source rate that maintained the submarine network as a collateral duty. The drawback to the latter is that the officer does not have a traditional communications experience. The benefit to the latter is that officer is actually better equipped to support submarine communications in its current and future IP based network configuration. It is uncertain where future generations of 6290 LDOs should originate. If the submarine force continues not to integrate with IP 1820 community, or send newly commissioned 6290 LDO officers for official IT/IA training, suitable manpower relief will have to originate from the new ITS rate. This may become problematic because there are no submarine IP/IT/IA officers.

When a new ITS Chief who has no experience with traditional submarine communications but was a prior Sonar Technician (ST), Fire Control Technician (FT), or Navigational Electronics Technician (NAVET), desires to submit a commissioning package for 6290 LDO, it is currently unknown how the officer selection board will view the Sailor's contribution to the 6290 LDO community. With no experience in traditional submarine communications, it is doubtful that the Sailor will be selected for 6290 LDO. The submarine force must have a plan for new officers commissioning from the new submarine ITS rate. The current LDO recruiting brief does not address the ITS rate as a future officer source.

Feasible solutions requiring further research:

- Assign communications 6290 LDOs to at sea submarine duty as junior officers. This will put the submarine force back on track and further lay a proper foundation for solid cyber security in the future.

- Combine the submarine communications division and ITS division and send new communications ETs to more IT schools. Communications ETs are already receiving some IT training at A-school. Currently, TYCOM senior communications department heads are reluctant to tackle such a significant task.
- Create a submarine IT Chief Warrant Officer (CWO). The submarine force is no longer producing submarine electronics CWOs due to obsolesce of that particular Officer designator. The vitality of a submarine IT CWO could be a cost effective option for an IA/IT manager for ISIC and some afloat platforms.
- Establish a new IA/Security subject requirements manager position at the ISIC or Group Commander level. This position can be filled by a 6290 LDO or civilian equivalent. This new position would:
    - Initiate related tiered training at the ISIC level to train and transition a management solution to ISIC staff and subordinate afloat units
    - Review current IA requirements and status of related documentation at the afloat command level to establish a status baseline among subordinate afloat units
    - Establish a liaison with DoD / DoN level authorities at ISIC level

D. IA REQUIREMENTS MANAGER

The proposed IA requirements manager solution approach is intended to incorporate detailed/system TYCOM, ISIC and afloat command specific information of GENSER and DoDIIS IA requirements, providing a Secure Internet Protocol Router Network (SIPRNET) based single point of reference facilitating visibility and proactive management of all IA requirements at all levels of submarine force command. The current IA management architecture is disjointed and does not follow a proper administrative chain of command. The proposed IA management architecture (Figure 8) is more appropriate and will incorporate detailed systematic TYCOM, ISIC and afloat command specific information of GENSER and DoD Intelligent Information System (DoDIIS) IA requirements, providing a SIPRNET based single point of reference,

facilitating visibility and proactive management of all IA requirements at all levels of submarine force command.

In addition, the Department of Defense (DoD) Intelligence Information Systems (DoDIIS) is the authoritative technical and management architecture for management of all systems processing Top Secret-Special Compartment Information (TS-SCI) information.

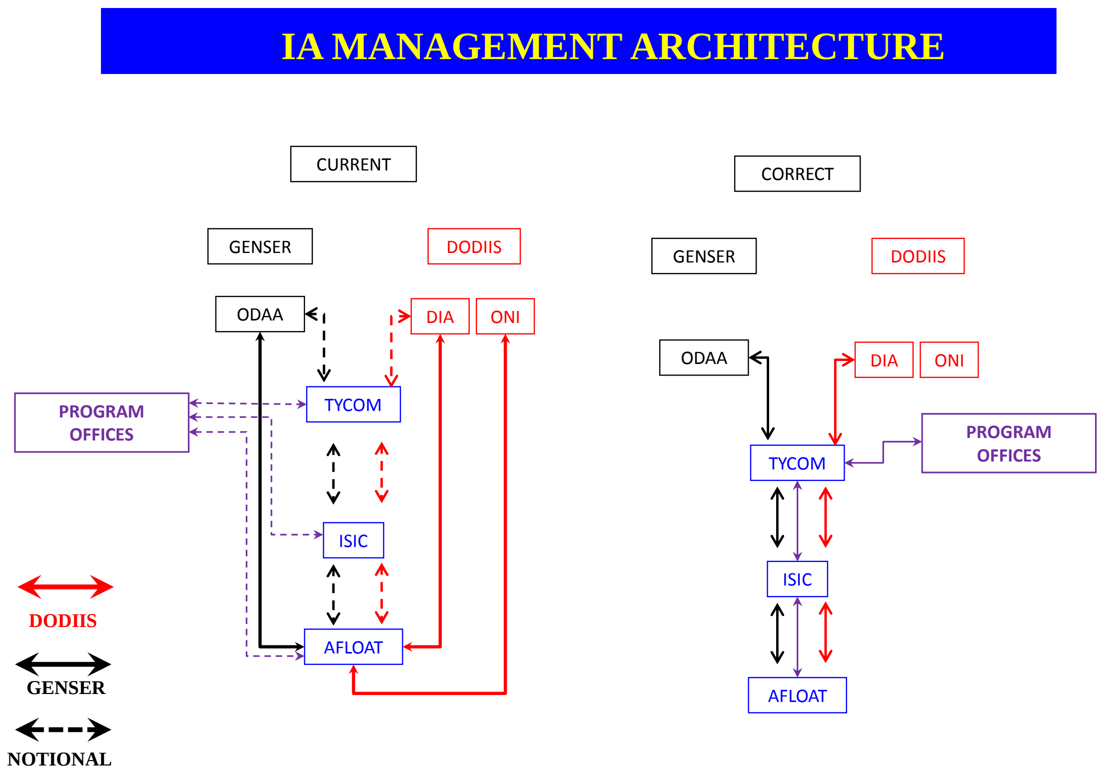

Figure 8. IA Management Architecture

E. SUMMARY

IA requirements levied across the DoD and related domains continue to evolve, increasing in number and complexity. The impact of this at the afloat/tactical command level culminates in a significant impact in the ability to effectively manage these

requirements. Without a management solution, coupled with the limited ability to obtain and maintain the requisite IA and related skill sets at this level, what is created is an increased threat to data, systems, networks, significant expenditure of associated resources/man hours and overall mission capability. The submarine force already maintains an experienced officer corps that requires additional IT/IA training. In order to support to the full potential of the intent of DUSW, the return of the submarine Warrant Officer directly commissioned from the ITS rate will pay priceless dividends for the submarine force.

The proposed IA requirements manager (officer or civilian) solution approach is intended to incorporate detailed/system TYCOM, ISIC and afloat command specific information of GENSER and DoDIIS IA requirements, providing a Subject Matter Expert (SME) based single point of reference facilitating training, visibility, and proactive management of all IA requirements at all levels of submarine TYCOM, ISIC and afloat command level. General Service (GENSER) requirements are applicable to systems processing for CONFIDENTIAL, SECRET, TOP SECRET, and Special Compartment Information (SCI) level information. An additional, commonly overlooked, duty of an IA requirements manager should be establishing and maintaining an administrative risk assessment program for the submarine networks. Even a basic qualitative risk assessment process for the Commanding Officer and ITS division would provide understandable mitigations for network vulnerabilities.

IX. RISK ASSESSMENT

A. BACKGROUND

Risk assessment is a phrase that is often used in the submarine force and is equally misunderstood. Risk, as lectured during a Naval Postgraduate School risk management lecture, is the potential of losses and rewards resulting from an exposure to a hazard or as a result of a risk event. "Risk management is the act or practice of dealing with risk. It is a process used to plan for risk, assess (identify and analyze) risk areas, develop risk handling options, monitoring risks to determine how they have changed and documenting the overall risk program" (Department of Defense Risk Management Guide, 2006, 7). In other words, risk assessment should be managing what can go wrong, determining how likely is it to go wrong, and deciding what happens if it does go wrong. As another definition of risk puts it this way: "Risk is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur" (Guide for Conducting Risk Assessments 800–30 Rev1, 2012, 12). "The purpose of risk assessments is to inform decision makers and support risk responses by identifying: relevant threats to organizations or threats directed through organizations against other organizations; vulnerabilities both internal and external to organizations; impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and likelihood that harm will occur" (NIST 800–30 Rev1 2012, ix). For submarine IT managers, "Risk assessments are a key part of effective risk management and facilitate decision making at all three tiers in the risk management hierarchy including the organization level, mission/business process level, and information system level" (NIST 800–30 Rev1, ix). In this context, the *mission/business* is the protection and strengthens Information Assurance on submarine networks.

B. INFORMATION ASSURANCE AND RISK MANAGEMENT

The *National Institute of Standards and Technology (NIST) 800–37* is a "guide for applying the Risk Management Framework to Federal Information Systems" (NIST 800–37 2010, 2). The *DoD Risk Management Guide for Acquisition*'s purpose is to "assist

DoD and contractor Program Managers (PMs), program offices and Integrated Product Teams (IPTs) in effectively managing program risks during the entire acquisition process, including sustainment" (DoD RMG 2006, i). At the Navy level, there is the *Navy Information Assurance* (IA) *Program* OPNAV 5239.1C, the Navy IA program instruction that establishes policies and procedures for the Navy's Information Assurance (IA) program. OPNAVINST 5239.1C does not contain any risk management guidance at the TYCOM level or below. Anything further down towards the TYCOM level and afloat unit, and there continues to be no risk IA Risk Management (IARM) program in place. A thesis by Lambert was published in 2002 on Information Risk Management (IARM) , and in it, he attempted to establish "a method to standardize the Department of the Navy (DoN) human factors involvement in information assurance Navy-wide, (2) and determine if it necessary for a specific IARM course and at what level" (Labert 2002, V) In particular, Lambert's research asked, "at what level would an IARM course be appropriate: an afloat unit? Squadron? Group? or TYCOM?" (Labert 2002, V)

Lambert conclusions suggest that a TYCOM, in partnership with a SUBLAN Program Manager, establish a simplified operational level risk assessment training program for each submarine to analyze the ship's overall network vulnerabilities. This risk management program would measure the impact on the ship due to the loss of part or all of functionality by determining the probability and identification of controls and safeguards that can reduce the operational risk to an acceptable level. Before any risk training program or risk application can be used onboard, a basic understanding of the two basic types of risk analysis should be considered: qualitative and quantitative. A qualitative risk analysis assessment may be the better then a quantitative analysis at the afloat level, due to the qualitative risk assessments conducted by onboard subject matter expert, whose experienced opinions and collective judgment makes it possible to evaluate the probability, consequence or severity, and likelihood values.

C. UNDERSTANDING RISK ANALYSIS

To support a risk assessment, a risk analysis is necessary to determine the inherent risks, including both the internal and external environments in addition to the Information

Systems (IS) risks onboard. Submarine network security can be threatened by various agents with a variety of means. IT management is charged with showing that due diligence is performed during the decision-making processes regarding the effect on ships' network with respect to the level of risk mitigated, identification of threats, and the impact of a threat. A formal risk analysis provides the documentation that due diligence has been performed. An independent assessment from the submarines ISIC can offer an assessment of how their ships are performing. Unfortunately, there is no effective risk analysis available for submarine ITS personnel and command and control leadership to utilize in order to ascertain and define an acceptable level of risk for any submarine network not in compliance with any internal or external assessment performed.

Risk analysis should provide three main deliverables:

- identification of threats,
- determination of the probability and impact of a threat, and
- identification of controls and safeguards that can reduce the risk to an acceptable level. Each of these risk areas can be analyzed at the qualitative or quantitative level.

D. UNDERSTANDING RISK ANALYSIS AND CYBER-1

The closest attempt is in COMSUBFOR Cyber-1. CYBER-1 prescribes the minimum policies for network readiness and IA of Submarine Force networks. CYBER-1 refers to a risk assessment but utilizes a simple yes or no compliance checklist (COMSUBFOR 2011, 87). A simple yes or no compliance checklist cannot provide an effective quantitative risk analysis to analyze the ship's overall network vulnerabilities to measure the impact on the ship due to the loss of part or all of functionality. The current version of Annex A of CYBER-1 assessment checklists could be utilized to create a basic risk assessment if the DoD Risk Management Guide (Department of Defense RMG, 2006) and (NIST) 800–30 Rev1 (NIST 800–30 Rev1, 2012) are used as a basic starting point. The current Annex A of CYBER-1 is more administrative in nature and less technical in nature. No specific risk assessment checklist is included.

Annex A to CYBER-1 contains the following TABs for self-assessments:

- TAB A—Administration Checklist
- TAB B—Manpower Checklist
- TAB C—General Information Assurance Checklist
- TAB D—Network Configuration Checklist
- TAB E—Network Operations and Behavior Checklist
- TAB F—Physical Security Checklist (this TAB is not directly associated with network security and is also covered in the Department of the Navy security manual 5510.36)
- TAB G—Maintainability Checklist

(COMSUBFOR 2011, 87)

E. QUALITATIVE APPROACH

1. Likelihood

"The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities)" (NIST 800–30 Rev1 2012, 10). CYBER-1 or any other documentation researched does not support any weighted risk factors to be included in any analysis.

To derive an overall likelihood weighting that indicates the probability that a potential vulnerability may be executed within the associated threat environment, the following governing factors should be considered:

- Threat source, motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

Further research is recommended to identify specific "taxonomy of threat sources capable of imitating threat events" (NIST 800–30 Rev1 2012, D-1) onboard submarines.

In addition to the three items above, for submarine networks, the following should also be considered. Are the networks

- Currently connected shore side
- Currently at sea
- IAVA compliant

- Virus definitions compliant

It matters if a submarine is at sea or connected at the pier. Due to the nature of submarine connectivity while at sea, the biggest threat a submarine is concerned with is system administrator error, equipment fault, or an insider threat. In port, the submarine has to deal with all of the previously listed threats, with the addition of being connected to the Global Information Grid (GIG).

The likelihood that a potential vulnerability can be described as ranges from very low to very high, as shown in Table 1. After likelihood level is assigned to each checklist line item, a basic risk red, yellow and green stoplight chart could then be utilized, formalized and used for executive review. From here, the afloat command could generate their own basic risk management plan.

Table 1. Assessment Scale–Likelihood of Threat Event Occurrence (non-adversarial) (After NIST 800–30 Rev1 2012, G2)

Qualitative Values	**Semi-Quantitative Values**	**Description—Root cause**
Very High	9–10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	7–8	Error, accident, or act of nature is highly likely to occur; or occurs between 10–100 times a year.
Moderate	5–6	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1–10 times a year.
Low	3–4	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0–2	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

2. Quantitative Approach

For a quantitative measure more suitable of a standard format, a formal standard risk reporting matrix for evaluation and reporting of network vulnerabilities can used to determine the level of risks identified within each TAB of Appendix A in CYBER-1.

3. Severity and Consequence

In order to set the stage and understanding of the severity or consequence, each line item from each TAB of the compliance checklists should be considered an event and weighted with a severity or consequence between 0 and 10, with 0 being lowest impact and 10 being the most significant undesirable impact of that event. The severity rating and description should be broken down in the following fashion from Table 2.

Table 2. Assessment Scale–Vulnerability Severity (After NIST 800–30 Rev1 2012, F-2)

Qualitative Values	**Semi-Quantitative Values**	**Description—Root cause**
Very High	9–10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	7–8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	5–6	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	3–4	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0–2	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

4. Summing the Assessment

After recording the numerical results from Tables 1 and 2, the level of likelihood of each root cause should be assessed using Table 3. For example, if the root cause was estimated to have a 70% probability of occurring, the corresponding likelihood will be assigned Level 4.

Table 3. Levels of Likelihood Criteria (From DoD RMG 2006)

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~30%
3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

The sum of the assessment of TAB A checklist can then be plotted in a format for suitable for executive review, as shown in Figure 9.

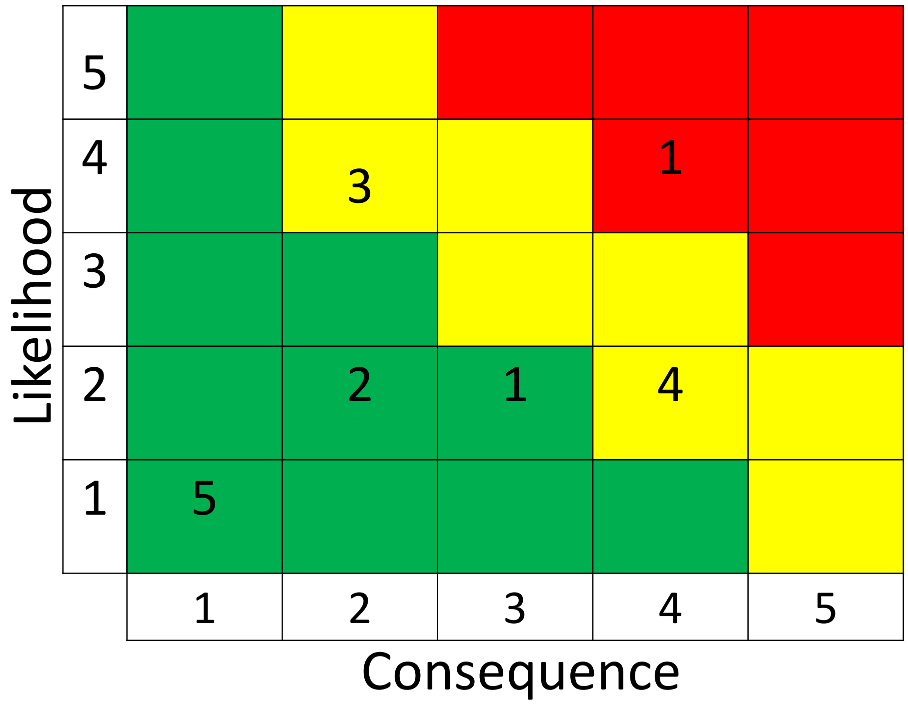

Figure 9. Risk Assessment Block

5. Impact

In the context of this report, risk is any loss affecting the total IA trade space consisting of training, confidentiality, personnel, integrity, equipment, and availability. Since the impact on IA is the focus, the following is used to describe the submarine network's loss in terms of the traditional integrity, availability, and confidentiality elements.

6. Loss of Integrity

System and data integrity refers to "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" (NIST 800–30 Rev1 2012, B-7). Integrity is lost if intentional or accidental unauthorized changes are made to the network affecting the overall Information Assurance level. This could happen at the user or system administrator level.

7. Loss of Availability

Availability is here defined as “Ensuring timely and reliable access to and use of information” (NIST 800–30 Rev1 2012, B-2). If a mission-critical IT system is unavailable to its end users, the organization’s mission may be affected by the loss of system functionality and its operational effectiveness. Loss of availability does not affect all classes of submarines the same way. The difference between a SSBN- ballistic submarine and a SSN/SSGN attack submarine is its mission. Their specific use of SUBLAN is very similar but use of other tactical networks is significantly different. Those differences are beyond the scope of this report.

8. Loss of Confidentiality

Confidentiality is here defined as “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” (NIST 800–30 Rev1 2012, B-3). The Navy mitigates loss of classified, privacy, and proprietary information through the employment of various software systems and administrative Information Systems security programs that cover areas from physical to personnel. Discussions of these programs are not within the scope of this paper.

F. THE TRAINING THREAT

The first issue to tackle is the training piece. The level of knowledge across the board is not as strong as it should be to outwit and outlast the outsider and insider threats. The formal school and on-the-job training process is underfunded and lacks rigor and strength. Formal education is needed at the administrators’ and users’ level. Training is like a ship: if not taken care of, the ship may end up being not sea-worthy. Therefore, the quality of the training is important.

G. THE EQUIPMENT THREAT

Another potential threat is the obsolescence factor where hardware and software updates are in dire need. The SSBNs finally moved off of WIN 2K as an operating

system. The new operating system is Windows XP, which is already outdated when compared to civilian standards. Red Team Assessments on SUBLAN on various submarine platforms have been conducted. The analysis points similar findings as the ones discovered in this paper, i.e., at the acquisition program level, current SUBLAN hardware and software is obsolete. Have the assessments made a difference in turning around the trends in training, resources, and culture within the SSBN community? The answers are yet to be known. Can the Navy afford to continue on the present course with the risks known and unknown, with the lack of accountability with the SUBLAN?

H. SUMMARY

1. Risking It All

As mentioned earlier, risk analysis has three main deliverables:

- identification of threats,
- determination of the probability and impact of a threat, and
- identification of controls and safeguards that can reduce the risk to an acceptable level.

The cyber workforce is the first line of defense and their understanding of Risk in relation to the security of the ships networks is vitally important. The Command and Control element should have the basic doctrine to provide a rapid development of the current level of risk the network may develop at any given time. The framework for this doctrine is currently available at the DoD level. The next step is to implement this framework down to the TYCOM and afloat unit level to keep our virtual submarine secure.

X. THE VIRTUAL SUBMARINE

In the cyber domain, the war is clearly "in progress" so to speak. It can be seen on the news, in the papers, on the Internet, and U.S. Government (USG) networks. The nation's cyber adversaries are working hard to penetrate USG networks. To assume that adversaries are not after operational and technical information and not trying to cause disruption to the Command and Control decision making process would be a gross conceptual error (COMSUBFOR 2011, 1).

The United States (U.S.) military should not be considered the only target. The defense industry and the government as a whole should also be considered at risk. Working towards a common goal of hardening the IA Defense-in-Depth boundaries will be the strongest defense and if necessary, the strongest offense. The current levels of training for U.S. sailors, while improving, are still inadequate to the task of having a sufficient level of IA for defense against cyber warfare. The submarine force has an inadequate level of knowledge and manpower in this area for both the submarine officer and enlisted communities.

Every submarine has physical brow for boarding. A person is required to

- show proper identification,
- ask for permission to come aboard,
- grant permission and then
- provide access to the submarine.

Sometimes, a person is escorted onto the submarine and is given limited access to sensitive areas.

Each submarine has a virtual brow as well, that spans from the ship's network to the outside world. Conceptually, this virtual brow's security controls should work the same way as the physical brow of the submarine, if not better. The security controls must work better because it is anticipated that the next major conflict for the U.S. military will not be using conventional warfare; it could be a virtual cyber conflict and one that is already in progress.

In order to change the mindset to grasp the concept of the virtual brow, the Submarine Force should strive to stop thinking about Information Systems solely as an oversight of SUBLAN, but rather expand the definition to include all the hardware, software, interconnecting systems, security controls, operations and maintenance processes that go into the movement of critical information from source to the decision-maker; in short, “End-to-End Security” that encompasses all layers of the Open Systems Interconnection OSI model and makes use of the Defense-in-Depth model. In the cyber domain, the ship is vulnerable if informational systems are not held to the same operational, maintenance, quality assurance, and defensive standards that would be applied to propulsion, ship control, weapons, navigation, combat, and the sailors who operate and maintain those ship systems.

For example, a well-run ship has a thorough zone inspection program. Every space is inspected; deficiencies are noted and corrective actions are taken. The virtual ship should be held to the same standard. Software applications that do not work should be considered as similar to other parts of the real ship that do not work. If the virtual ship were inspected at the same level as the physical ship, then software version control would be held to be as just as important as material configuration control. Maintaining the latest operating systems, applications, and so on would be a high priority, and so on. Old files on servers creating a digital landfill would be considered to be as problematic as physical trash building up in the operating spaces (COMSUBFOR 2011, 1).

The cyber domain presents clear and present risk to the USG and military operations and every maritime participant who shares information resources with the submarine force. Because of the wide-reach of the cyber-domain, then it follows that cyber domain security should be the business of commanders, and not completely be delegated to LAN administrators; commanding officers and executive officers need to ensure that an understanding of IT/IA Concept of Operations (CONOPS) is part of their knowledge base. The primary reason for this is that knowledge of IT/IA CONOPS relates directly to war fighting ability. Success will require the participation of every submariner. A deeper understanding of the virtual ship—where straightforward action, as well as

long-term vigilance is required—will set a new normal for IT operations, so as to strengthen the virtual brow in the cyber war-fighting domain.

A. SUMMARY

The virtual submarine did not exist a decade ago. However, the submarine force cannot dismiss the very real, asymmetric threat operating today. The dependence on the movement of information brings with it real responsibility to understand and to manage. In the cyber domain, as in every other war fighting domain, the Submarine Force must be ready (COMSUBFOR 2011, 1). While the principles that have been learned over the last few decades of operating submarines should apply to the virtual submarine as well, they do not; we continue to fall short of putting that theory to practice. Senior deckplate leadership should strive to grasp this new battlespace that takes place in virtual domain. This is not traditional warfare, and it may require nontraditional battle management techniques.

THIS PAGE INTENTIONALLY LEFT BLANK

XI. CONCLUSION

There are significant gaps in the United States Navy (USN) Submarine Force's ability to integrate and manage Information Assurance requirements (IA), Information Technology (IT) manpower, End-to-End security, IT equipment, IT training, and applicable documentation that meets the intent of the "Design for Submarine Warfare" initiative promulgated in July 2011 The DUSW's intent is to have a shared sense of main objectives, and to align multiple efforts." (Caldwell, Richardson, and Breckenridge 2011).

Furthermore, the Submarine Force lacks common criteria for IA integration as a system of systems (SoS), when such an SoS is defined as a structured methodology to standardize and document IA requirements, IT requirements management, IT manpower, end-to-end security paralleled with end-to-end reliability, IT equipment and training, IA physical/functional/behavioral network boundaries, and applicable documentation that meets the intent of the "New Design for Submarine Warfare" initiative.

The research addressed the questions of "How can the Submarine Force better prepare and improve its Information Technician (IT) personnel, equipment, and training to meet increasing submarine warfare requirements worldwide? How can this be accomplished while employing undersea forces and delivering future undersea warfighting capabilities without further unnecessarily sacrificing valuable monetary and manpower resources?"

Furthermore, this research analyzed the capability of the Submarine Force's "New Design for Undersea Warfare" (DUSW) initiative, described as the ability to "fight our virtual ship in the cyber domain as capably as we do in the undersea domain" (Caldwell and Richardson 2011, 4).

The aim of this research was to provide submarine combatant commanders, submarine type commanders, submarine squadron commodores, and submarine afloat commanding officers with an improved comprehension of the concepts necessary for the

Submarine Force's ability to fight the virtual ship in the cyber domain as capably as the undersea domain. The term *virtual ship* should not imply improved information systems but rather a comparison of warfare in a physical battle space of either land, air, or sea with the virtual concept of network warfare.

The following sections provide answers to the research questions and a comprehensive summary of findings and conclusions.

A. END TO END SECURITY CONCEPT

End-to-end security is complete data protection from writer to reader as the data travels through the entire OSI and TCP/IP model. Due to advancement in hardware/firmware, the easiest and most popular protection model is within a network's infrastructure. Simple network access via a token or common access card will not provide end-to-end security unless that model is applied and ends at application Layer 7. But, if protection is applied to the data from writer to reader and not just the communications infrastructure alone, then true end-to-end security starts and ends at (application) Layer 7, before data is sent on the network to the end user. Therefore, end-to-end security measures cannot be truly solved at any layers lower than that without addressing the entire OSI/TCP/IP model working together within the IA trade space as a System of Systems.

The development of the TCP and IP parallels the development of the OSI model. IP is connectionless and stateless which means that there's no sense of end-to-end connections. Packets of data can get lost for many reasons, but the connectionless nature of IP means that we have a dynamite ability to transparently add alternate routes and improve system availability.

IT operators and system administrators must understand the concept of end-to-end security so as to put in place necessary measures for a proper end-to-end security model. Lack of understanding of this concept by submarine network program managers inadvertently causes a lack of acquisition and policy support necessary to keep up with dynamic network security measures. Senior leadership should understand the end-to-end

security concept in order to understand the cause and effect on overall ship mission and support functions. They need to know what questions to ask and demand closure from TYCOM via the program managers.

B. TECHNOLOGY DRIVEN PRODUCT ARCHITECTURE

It is important to understand the advances in technology that have changed product architecture. That product was, and still is, the Internet and its ability to function the way it does. Normally a demand will drive a product to be developed for s specific purpose. In the case of the concept of the Internet as now known, advancement technology itself was the main driver behind the Internet architecture. This advancement in technology was felt in the Navy and submarine force and was well taken advantage of for the next step in the Navy and submarine force's Information Technology ambitions.

C. IT21 TO ITS

The Navy's IT-21 program was off to a good start with establishing a plan to modernize, standardize, and take advantage of the new networking technology that enabled Command to communicate in a non-traditional fashion with a non-traditional system that was maintained by non-traditional sailors as a collateral duty. IT-21 worked for many years until networking became less of a luxury and more of a requirement. IT-21 program was not updated as fast as technology and the demand for connectivity increased. Subsequently, the need for higher trained and dedicated operators, technicians, and officers also increased. Almost two decades later it became apparent that the concept of a new battlespace may exist and a new design to deal with that battlespace and revitalize traditional battlespace warfare was needed.

D. DESIGN FOR UNDERSEA WARFARE

DUSW is a plan to get the submarine force on a new dead reckoning course. Even with some minor shortfalls with DUSW addressing Lines of Effort for IA/IT/LAN systems, programs, and personnel, a deeper reach to leverage the proper level of experts already embedded in the submarine force will ensure the DUSW spirit of intent behind those LOEs.

E. INFORMATION ASSURANCE PHYSICAL, FUNCTIONAL, AND BEHAVIORIAL BOUNDARIES

The concept of IA boundaries as it relates to the DiD model and OSI model is relatively new suggestion. With a basic understanding of those models and IA, a direct correlation can be observed. With a basic understanding of IA and the operation of those systems that this research addresses, the concept of IA boundaries can be understood by operators, technicians, PMs, and leadership. IT operators and technicians are among the highest priority to understand this concept and manage all of the IA requirements management. But it will require new personnel, training, and leadership: a new human capital strategy. How will the submarine force build these enlisted ranks with the proper Navy Enlisted Education Code (NEC) and training while managing the overall manpower and resources for the submarine missions that rely on complex networks?

Through the study of Systems Architecture and reviewing IA holistically as a system of systems, IA boundaries can be identified. For example:

- Physical security layer is directly related to this physical IA boundary.
- The functional boundary correlates to the host security, internal network, and perimeter security Defense in Depth layers.

The behavioral boundary correlates to the data security layer that deals with application and data.

F. HUMAN CAPITAL STRATEGY

When reviewing this problem, it is possible to observe that there are two significant, but unofficial, types of submarine Information Technicians. The first type is the Information Technician who has been fully converted with the 2791 NEC, filling the Information Technician billet in accordance with the LAN stabilization message, but is being leveraged to work outside the LAN division supporting that sailor's division and rate; the LAN is treated as a secondary and collateral duty.

The second type of Information Technician is that sailor who is working in the Information Technician division either as a part-time collateral duty or full-time, but who is not a fully converted information technician. This is clearly poor personnel

management, due to observations previously mentioned above and misplaced contributions by sailors being tooled and used for one job, yet being tested and advanced in rate in which they have not functioned for an extended period of time. The author of this thesis can only observe this is a lack of sensitivity to a core group of sailors forced to take care of the ship's network; what once was considered a collateral duty has become a full-time job. However, this task is still *treated* as though it is a collateral duty. Needs, requirements, and functions must synchronize.

G. IA REQUIREMENTS MANAGEMENT

IA requirements levied across the DoD and related domains continue to evolve, increasing in number and complexity. The impact of this at the afloat/tactical command level culminates in a significant impact in the ability to effectively manage these requirements. Without a management solution, coupled with the limited ability to obtain and maintain the requisite IA and related skill sets at this level, what is created is an increased threat to data, systems, networks, significant expenditure of associated resources/man hours and overall mission capability. The submarine force already maintains an experienced officer corps that requires additional IT/IA training. In order to support to the full potential of the intent of DUSW, the return of the submarine Warrant Officer directly commissioned from the ITS rate will pay priceless dividends for the submarine force.

The proposed IA requirements manager (officer or civilian) solution approach is intended to incorporate detailed/system TYCOM, ISIC and afloat command specific information of GENSER and DoDIIS IA requirements, providing a Subject Matter Expert (SME) based single point of reference facilitating training, visibility, and proactive management of all IA requirements at all levels of submarine TYCOM, ISIC and afloat command level. (General Service/Collateral (GENSER) requirements are applicable to systems processing for CONFIDENTIAL, SECRET, TOP SECRET, and Special Compartment Information (SCI) level information. An additional, commonly overlooked, duty of an IA requirements manager should be establishing and maintaining an administrative risk assessment program for the submarine networks. Even a basic

qualitative risk assessment process for the Commanding Officer and ITS division would provide understandable mitigations for network vulnerabilities.

H. RISK MANAGEMENT

Risk analysis has three main deliverables:

- identification of threats,
- determination of the probability and impact of a threat, and
- identification of controls and safeguards that can reduce the risk to an acceptable level.

The cyber workforce is the first line of defense and their understanding of Risk in relation to the security of the ships networks is vitally important. The Command and Control element should have the basic doctrine to provide a rapid development of the current level of risk the network may develop at any given time. The framework for this doctrine is currently available at the DoD level. The next step is to implement this framework down to the TYCOM and afloat unit level to keep our virtual submarine secure.

I. THE VIRTUAL SUBMARINE

The virtual submarine did not exist a decade ago. However, the submarine force cannot dismiss the very real, asymmetric threat operating today. The dependence on the movement of information brings with it real responsibility to understand and to manage. In the cyber domain, as in every other war fighting domain, the Submarine Force must be ready (COMSUBFOR 2011, 1). While the principles that have been learned over the last few decades of operating submarines should apply to the virtual submarine as well, they do not; we continue to fall short of putting that theory to practice. Senior deckplate leadership should strive to grasp this new battlespace that takes place in virtual domain. This is not traditional warfare, and it may require nontraditional battle management techniques.

J. GOVERNANCE

Organizational governance must raise the level of awareness as to network security protection. In this case, protection means the IA on the devices that store, manipulate and transmit information through equipment, people and procedures. Security is a discipline that starts with ethics and training. The organization, or Command, should take the responsibility to set ethical behavioral standards and train shipboard personnel so that they understand the standards as set forth by the leadership. These standards can, therefore, be reflected in the next update of the Design for Undersea Warfare.

Training, personnel, and equipment, along with confidentiality, integrity/authenticity, and availability of information should connect with ethics and security practices for total End-to-End Security. Organizations need to set solid IA policy that outlines how an organization collects, uses, and protects the data stored within the *digital landfill* for command and control information. An independent broker, trusted agent, or IA requirements manager could provide the needed assurance that information from submarines will be re-protected. Otherwise, the course submarine security is on could manifest into a situation that could cost DoD and the DoN a significant amount of money to correct.

K. PERSONNEL

There will be high costs to not correctly presenting the consequences if submarines fail in their due diligence in providing adequate training, resources, and security. Moreover, organizational leadership must realize that information security is a daunting challenge and that it is more than an Information Technology (IT) departmental issue. Awareness and understanding of Information Security issues must permeate all decisions and all ranks of the organization and not just the IT department. A paradigm shift in watchstanding must take place because submarine IT duties are no longer a collateral duty. Submarine communications division and ITS division merging will produce nothing but benefits and solve the manning, watchstanding, and organizational

challenges. The senior enlisted leadership and senior communications officer leadership must lead this effort with command and control element support.

Self-monitoring could be centralized and coordinated through an independent broker offering up various products and services to optimize the well-being of IS including the security and protection of vital information that will enable submarines to meet their missions today and tomorrow.

When Program Managers, Chief System Engineers, fleet representatives, et cetera think about acquisition requirements for IT/IA/LAN, interoperability to meet capability continues to miss the mark or is not considered an acquisition target when viewing IT architecture as a system of systems.

L. AUTONOMY VS. MANAGEMENT

Bits are bits and they go down the wire or over the either at the same speed regardless of whether they are administrative or tactical bits. So the problem has everything to do with an organization weighed down by bureaucracy, which in this case means the Submarine Force's inability to adapt. The Submarine Force has not operated autonomously since reliable satellite data communications became the norm. Within one sailor generation later, networking became the norm and command and control changed again.

In the corporate military, there is a very strong impetus to control and in many instances, that is the military's job. But, often this controlling function means that the military, that means "manage," with a very narrow practical definition. It ends up coming out as "we do not allow anything on the network that we have not approved" (meaning purchased).

This is a long way from reality in a civilian or industry setting. The concept that seems to be missing as this high level discussion heads into uncharted waters is interoperability. Interoperability is orthogonal to ownership. There is no real need to own something to use it. A component does not need to be owned for it to be interoperable with the rest of the IT and communications infrastructure. Further, ownership does not mean the owner now has something interoperable. That would be viewed as a total non-sequitur, meaning:

- none of the solutions match the problem
- executing the solution will, again, cause an unproductive turf war adding to the current ones.

M. PLATFORM ABILITY

Additionally, the problem viewed here can be a cross-platform service problem. Every information system or system that is of any real interest involves cross-platform service from one platform or service to another. But the entire military procurement system is more oriented on acquiring platforms, not cross-platform sections. Changing the platform-oriented habits of a few decades probably will not happen. But we can, for a whole lot less effort and hassle, get the IA interoperability part right. This is where command and control element, at the Commander O5 and Captain O6 level, along with our industry engineering partners are important. A more cohesive interface between the TYCOMS and the acquisition corps is needed.

THIS PAGE INTENTIONALLY LEFT BLANK

XII. RECOMMENDATIONS

The following recommendations are intended for ITS personnel, senior afloat leadership, ISICs, TYCOM, and Program Managers (PM) of IT systems onboard submarines. Some recommendations are administrative in nature while other recommendations are intended for PM level research. Recommendations that are conceptional in nature should be considered for the next review of DUSW.

Execute a thorough inspection of our virtual submarine evaluating the content created on all networks and stand-alone systems. This must include portable workstations, all removable media, IT personnel training, IT personnel manpower, and so on. This effort should reduce exposure to vulnerabilities to a minimum by eliminating all unnecessary and out dated data; reduce and eliminate the digital landfill.

Ensure that the classification of information is consistent with the classification limits of network upon which they reside. If the source is in question or cannot be found, proper research should be conducted at all levels.

Minimize downloaded portable media. Store classified data on shared network resources instead of local workstations or individual user accounts.

Evaluate processes for maintaining and transferring control of classified material for both electronic and physical.

Formalize, standardize, and utilize end-to-end security concept.

Redesign how formal schooling for IT fundamentals is administered. Training is critical to core competencies. Identifying the Submarine Force's IT competence in maintaining its networks and assessing risk to virtual ships is paramount.

Treat network hardware configurations and software environment as part of the weapons battery. Configuration enforcement is critical.

Leverage groups and squadrons in supporting afloat commanding officers in the virtual ship domain identical to traditional core competencies with respect to with

waterfront expertise, monitoring, and forceful backup. This required assessment and management of staff competencies is an investment to bridge gaps in shipboard Information Assurance processes and administrative programs.

Training should be initiated by TYCOM for officers and other leadership personnel in the CO/XO/NAV pipeline. They should also ensure requisite IT and IA knowledge, skills, and abilities are part of the newest schools. They should also provide the force with the policy, best practices, and supporting products to assist commanding officers and others who are accountable for the readiness of the virtual submarine.

The force should be provided with an authorized, and useful, list of approved software applications allowed, and there should be a formal process for updating the list. This long list should not be created without proper level of stakeholder involvement. TYCOM should create an IT governance board at the Squadron and Group level for the sole purpose of pulling fleet requirements and issues up to the echelon two and three level.

It is recommended further research and trade studies be conducted for end-to-end security solutions onboard submarine networks such as SUBLAN. The use of Public Key Infrastructure (PKI), Common Access Card (CAC), or similar token access card used in conjunction with the proper application will provide end-to-end security at all layers of the OSI and TCP/IP model. This will not only prevent loss of sensitive information via loss of data, but make it easier to mitigate the insider threat.

It is recommended further research be conducted to insert end-to-end security training into the submarine ITS training pipeline. Currently, the only network security training is the necessary material to obtain the Security Plus certification.

Two significant recommendations can be summarized from above:

1) All operational and administrative applications that attach to the Internet such as IT21, NMCI, ONENET etc..., should authenticate the data they use. No application should emit data that is not digitally signed. No application should naively (without warning the user) accept data that is not signed.

2) No application should emit classified data except in encrypted form. (in this context, application and end system should be considered synonymous. An example is encryption of e-mail messages. An incorrect example is relying only on VPNs.

A. FEASIBLE SOLUTIONS REQUIRING FURTHER RESEARCH

Assign communications 6290 LDOs to at sea submarine duty as junior officers to act as Information Operations officers. This will put the submarine force back on track and further lay a proper foundation for solid cyber security in the future.

Combine the submarine communications division and ITS division and send new communications ETs to more IT schools. Communications ETs are already receiving some IT training at A-school and ITS students are already receiving basic communications training as well. Currently, TYCOM senior communications department heads are reluctant or ill equipped to tackle such a momentous task.

Create a submarine IT Chief Warrant Officer. The submarine force is no longer producing submarine electronics Chief Warrant Officers CWO due to obsolesce of that particular Officer designator. The vitality of a submarine IT CWO could be a cost effective option for an IA/IT manager for ISIC and some afloat platforms.

Establish a new IA/Security subject requirements manager requirements manager position at the ISIC or Group Commander level. This position can be filled by a 6290 LDO or civilian equivalent. This new position or the CWO position would:

- Initiate related tiered training at the ISIC level to train and transition a management solution to ISIC staff and subordinate afloat units
- Review current IA requirements and status of related documentation at the afloat command level to establish a status baseline among subordinate afloat units
- Establish a liaison with DoD / DoN level authorities at ISIC level

Identify specific “taxonomy of threat sources capable of imitating threat events” (NIST 800–30 Rev1 2012, D-1) onboard submarines.

Capture reliability data to provide sufficient context to provide an effective standard of evaluation of in-use combat system software and hardware build.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

A. SUBLAN AND COMMON SUBMARINE RADIO ROOM ONBOARD ARCHECTURE

This appendix is provided for supplemental information. The SUBLAN has evolved into a ship-wide network infrastructure that provides connectivity throughout the submarine and enables submarine subsystems to interact with off-board entities via the Exterior Communication Subsystem (ECS). The SUBLAN subsystems includes networks and other services requiring interconnecting subsystems, as well as providing fiber optic cables and networking services that are required within subsystems. SUBLAN implements a SECRET-High Classified LAN and a separate Unclassified LAN. The Unclassified LAN is used primarily for Non-Classified Internet Protocol Router Network (NIPRNET) access to support administrative functions and quality-of-life related elements. The Secret LAN provides Secret Internet Protocol Router Network (SIPRNET) and supports a variety of Secret (and below secret) level tasks.

The basic configuration of SUBLAN provides network infrastructure, including an Unclassified Wireless LAN (UWLAN, *currently not allowed*), servers, and the Common PC Operating System Environment (COMPOSE), which provides the server and operating system environment for other applications such as Non-Tactical Data Processing (NTDPS) and Naval Tactical Command Support System (NTCSS).

The SUBLAN Classified and Unclassified networks connect to off-hull elements via the Common Submarine Radio Room's (CSRR) Automated Digital Network System (ADNS) Router, which provides both RF links and links for pier side connections.

The ADNS Hub consists of the two Main Routers in CSRR, which are the connecting point between the SUBLAN and CSRR.

The Ashore side piece delineates the major elements of the submarine message and electronic mail flow connectivity between the SSBN and the Broadcast Control Authority, Naval Telecommunications and Master Station Pacific (NCTAMS PAC), and the rest of the world.

The submarine input comes into the Very Low Frequency (VLF) receivers onboard and transmitters ashore. After processing through the routers and Policy Router, the electronic mail, messages, and other information are sent via shore-side to either the SIPRNET or the NIPRNET.

APPENDIX B

A. DESIGN FOR UNDERSEA WARFARE

This appendix is provided for supplemental information.

The work of our Undersea Force is complex, dynamic and vital to national security. With a community as broad and diverse as ours, it is important for us to have a shared sense of our main objectives, and to align our efforts to achieve them. The Design for Undersea Warfare serves these purposes.

The Design for Undersea Warfare is intended to be specific enough to clearly define the objective, while being flexible enough to encourage initiative and boldness throughout the force—at all levels—in the attainment of these goals. As such, it has implications for major commanders, facility commanders, submarine commanding officers, and each of our officers and Sailors.

Main Objectives: We will be masters of the undersea domain, able to achieve undersea superiority at the time and place of our choosing. We will be the experts for all matters in undersea warfare. Consistent with decades of past performance, our Undersea Force will apply itself along three main lines of effort:

- **Ready Forces:** Provide undersea forces ready for operations and warfighting
- **Effective Employment:** Conduct effective forward operations and warfighting
- **Future Force Capabilities:** Prepare for future operations and warfighting

It is difficult to separate warfighting from peacetime operations, as they are so closely related. Our undersea forces conduct peacetime operations to prevent war, by deterring and dissuading our adversaries and by assuring our Allies and partners.

Peacetime operations further serve to help us understand and shape the

battlespace, and to learn the capabilities of potential adversaries. Our goal is that by virtue of our robust and focused operations, we will clearly be ready to prevail in any conflict. The warfighting readiness and effectiveness of our Undersea Force should serve to compel potential aggressors to choose peace rather than war, restraint rather than escalation, and termination rather than continuation.

Enduring Attributes: What has not changed is that the success of our undersea forces depends on dedicated, technically skilled and engaged warriors.

Areas for Greater Emphasis: There are a number of long-term national security trends that interact to make undersea operations and warfighting capability increasingly important. In light of this, you will find several Focus Areas singled out for renewed dedication within our force. First, there is increased emphasis on the development and certification of relevant warfighting skills at the unit level, at the tactical and operational commander level, at the strategic level, and at supporting commands. Next, you will find increased emphasis on creativity and innovation, sparked by initiative and a heightened sense of authority, responsibility, and accountability at the lowest capable level—even to the individual.

This document defines our way forward in a complex and often unpredictable environment. As such, it will evolve—it is not a rigid plan. To ensure that necessary changes can occur, the Design for Undersea Warfare has assessment and learning built in—we will make changes as necessary.

The Design for Undersea Warfare is a framework for action. Read it, think about it, discuss it and act on it.

R. P. BRECKENRIDGE	J. F. CALDWELL, JR.	J. M. RICHARDSON
Director	Commander	Commander
Submarine Force	Submarine Warfare	Submarine Force
Division	U.S. Pacific Fleet	

Part I

Context for the Design

Assumptions about the world, key trends, threats

1. A chaotic and disorderly global security environment will increase demands on the U.S. Navy and U.S. Undersea Forces.

2. Globally proliferating submarines are increasing pressure on freedom of the seas and contesting our undersea superiority.

3. Anti-access, Area Denial (A2/AD) systems challenge our surface and air forces, placing increased responsibility on our undersea forces to enable Assured Access for the Joint Force.

4. America's vital undersea infrastructure (energy and information) is becoming even more critical and more vulnerable.

5. Our shrinking submarine force size requires that each platform must individually support more requirements across a broader area.

6. Deterrence provided by our stealthy, agile, persistent and lethal submarines (SSBNs, SSNs and SSGNs) will remain important against both state and non-state actors.

7. Ubiquitous media presence means we will need to exploit our concealment to provide our leadership options by remaining undetected and non-provocative when desired.

8. The expanded decision space that undersea forces provide will be increasingly valued by senior leadership as the security environment grows in complexity, leading to increased requests for undersea support.

Assumptions about the future

1. The operational environment will become more complex, further stressing the human element in undersea operations and warfighting.

2. Adaptive, determined and tenacious adversaries will exploit our weaknesses with little or no notice.

3. Survivable U.S. SSBNs will provide nuclear deterrence for the United States and many of our allies for the foreseeable future.

4. Combatant Commanders will continue to value the unique capabilities

and conventional deterrence that SSNs and SSGNs deliver.

5. Unmanned underwater system technology will advance with increased endurance and capability.

6. We will need to fight our "Virtual Ship" in the cyber domain as capably as we fight in the undersea domain. We must protect our information and our systems from attack and take the fight to the enemy.

7. Available financial resources will decrease due to budget pressures.

Expectations others have of our Navy and Undersea Forces:

We will be expected to achieve undersea superiority at the time and place of our choosing.

1. We will use the Navy to gain access despite diplomatic, geographic, and military impediments. (CNO)

2. We will build appropriate Navy force structure and provide it with an appropriate strategic lay-down. (CNO)

3. We will provide forces ready for tasking to Combatant Commanders. (USFF)

4. We will sustain our forces through their Expected Service Life. (USFF)

5. We will reduce Fleet overhead and fund deployable units at a higher priority than everything else. (USFF)

6. We will win wars, deter wars, defeat terrorists, and ease disasters with our Maritime Forces (Cooperative Strategy for 21st Century Sea Power)(CS-21)

7. We will secure the U.S. from attack; secure strategic access and retain global freedom of action. (CS-21)

8. We will provide persistently present, combat-ready Maritime forces capable of forcible entry and quick response to other crises. (CS-21)

9. We will impose local sea control wherever necessary -- by ourselves if we must.

(CS-21)

10. We will maintain nuclear weapons safety and security.

11. We will maintain nuclear reactor safety and security.

12. We will maintain security of classified material and information systems.

<u>Priorities—Enabling Success and Managing Risk</u>

1. Peacetime Operational Priorities:

- Safety: Our operational responsibilities hinge first and foremost on enforcing the highest standards of safety, including the prevention of collision, grounding, serious injury or death.

- Stealth: Safety is closely followed by a commitment to remaining undetected as we execute highly sensitive missions in support of our Nation's security. We must prevent counter detection, compromise of mission details, or exploitation of our sensitive classified information.

- Mission Aim: Mission accomplishment within the bounds of safety and stealth is our highest priority

2. Professional Behavior: We must embody the highest standards of character. At sea, we will conduct ourselves as proud warriors, worthy of bearing arms in the defense of our nation. Ashore, we will be ambassadors of the Nation and the Navy, preventing liberty or public incidents at home or abroad. The Commanding Officer must set a powerful example.

What We Must Do: Forces that support our efforts

Our people are the key to our success. The shared "Submarine Culture" running through our undersea community is our strongest supporting force. It provides us with our warfighting focus and our operational readiness. It must NEVER be compromised.

Alignment: Our value as a Force is significantly enhanced when we maintain a coherent alignment amongst our senior leadership and with each other. We must ensure we remain consistent both with our broader strategic responsibilities to the Navy and with the other elements of the Undersea Force.

Warfighting:

- We expect to operate and fight far forward, independently, "behind enemy lines," for long periods of time, without support

- We maintain ourselves as ready as possible to leave soon, move quickly and be among the first to penetrate the enemy's defenses

- We know our potential adversaries and have operating experience in the environments that might become future undersea battlegrounds

- We exploit concealment by the sea as a key to our success, but we respect that the same sea will kill us unless we hold it at bay

- We depend on stealth, surprise and boldness and practice these

every day. We safeguard tactical information and avoid exploitable patterns

- We understand that operating undersea is inherently a dangerous business and that only trained and vigilant individuals and teams will keep our ships and crews safe

- We understand “calculated risk” but avoid “unnecessary risk” by thinking ahead, anticipating risk and taking mitigating actions

Readiness:

- We stay ready to operate far forward on short notice by managing manpower, training and maintenance to avoid fluctuating readiness
- Our people are the backbone of our success. Submariners are national treasures.
- We have small crews. Each person has multiple roles. All are responsible for the ship’s safety, stealth and mission
- We depend on initiative, de-centralized command and teamwork
- We depend on absolute integrity. We employ back-up and second checks, but each person remains individually responsible.
- We comply with procedures, founded on technical understanding
- We know and use the source requirements and references
- We have no peer in our aggressive approach to improvement through assessment and training
- We candidly face the facts—good and bad—and proceed based on well-known standards that are based on thorough analysis.
- We ensure nobody is indispensible by building depth of expertise
- We incorporate safety and effective work practices into our habits
- We are resourceful. We always have a Plan B, and we can often fix the equipment even if we lack the parts
- We own our ships, taking meticulous care to maintain them in a state of maximum possible material readiness—ready to go to war

What We Must Avoid: Forces that work against us

1. Our current approach to inspections and assessments rewards cyclic and temporary narrow excellence instead of excellence which is sustained and broad.

2. Our TYCOM and ISIC efforts tend to limit a Commanding Officer's

freedom and flexibility. Shared responsibility and accountability between the ship and the chain of command is limiting CO's ability to achieve success. Excessive administrative distractions are burdensome.

3. We lose sight of the fact that warfare is a human-centric problem.

Insufficient emphasis is given to developing creativity and initiative, both of which are essential to the practice of de- centralized command upon which effective undersea warfare is based.

4. Our solutions to problems can tend towards bureaucratic, process- dominated approaches.

Part II Summary of the

Design for Undersea Warfare

Three Lines of Effort with Associated Focus Areas

Our undersea force has long approached its responsibilities for securing national security along three Lines of Effort (LOEs), depicted in Figure 1. The Design for Undersea Warfare also identifies associated Focus Areas, which describe the emphasis required within each LOE.

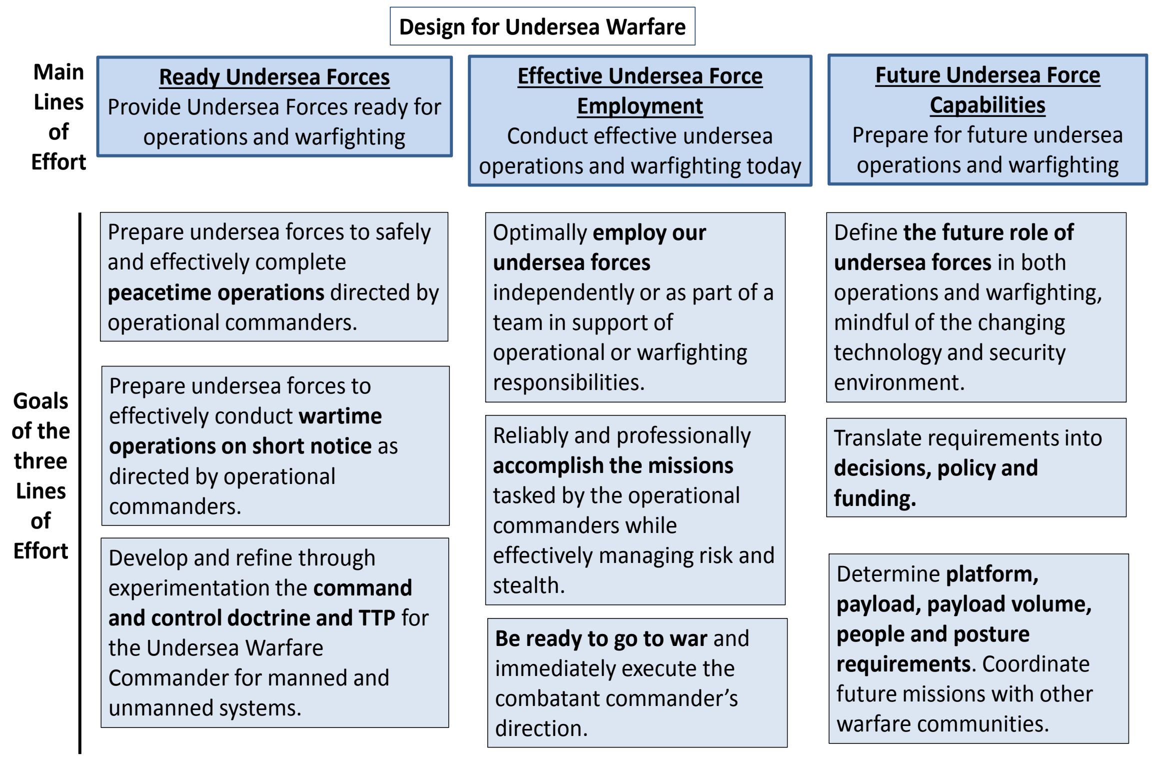

Figure 1 - Design for Undersea Warfare Lines of Effort

Each of the three Lines of Effort has associated Focus Areas:

<u>Ready Forces -- Provide Undersea Forces Ready for Operations and Warfighting:</u>

This captures our responsibility to prepare undersea forces for scheduled or emergent deployments as well as warfighting. The time horizon for this Line of Effort is roughly five years.

Focus Areas:

- **Enhance CO initiative and character**, including the responsibility, authority, and accountability to prepare the ship for operations and warfighting; structure the relationship with Squadrons, Groups and Type Commanders to shift the responsibility for preparation, planning, execution, assessment and improvement more to the ship. Maximize CO effectiveness by nurturing character and integrity at every opportunity.

- **Sustain warfighting readiness** during the inter-deployment period; adjust the interaction within the chain of command to reward stable, broad excellence vice short-term, cyclic pulses; return tactical initiative to the operating forces

- **Develop Undersea Warfare Commander Doctrine and TTP;** integrated

C2 for both manned and unmanned undersea systems; practices for effective coordination of mixed undersea forces with other forces

<u>Effective Employment -- Conduct Effective Undersea Operations and Warfighting</u>:

This captures our responsibility to work with operational commanders to be ready to establish undersea superiority at the time and place of our choosing.

Effectively employ undersea forces to reliably and professionally deliver the operational and warfighting performance expected by the Combatant Commanders.

The time horizon for this Line of Effort is roughly five years.

Focus Areas:

- Active engagement with Fleet and Operational Commanders to develop coordinated theater specific campaign plans that optimally employ our undersea forces; enhance development of innovative strategic and tactical employment of undersea forces (e.g., C7F Submarine Campaign Plan and supporting CSP Submarine Response Plan); tighten our assessment processes with Operational Commanders and supporting players to make us more effective warfighters.

- Increase the **deliberate and planned demonstration of warfighting capabilities** and access at the submarine and force level enhancing confidence in our abilities and systematically proving we can do what's required; lead in development of Theater USW Doctrine and teamwork; improve Mission Assurance to ensure we can fight through a range of C4I challenges in peacetime and war

- **Improve operational availability of undersea forces** while forward (through improved resilience, achieve better reliability, on-board repair, in-theater repair)

Future Force Capabilities -- Prepare for Future Undersea Operations and Warfighting:

This defines the future role of undersea forces, the associated requirements for platforms, payloads, manpower and operations, and the decisions, policies and resourcing required.

The time horizon for this Line of Effort is roughly five years and beyond

Focus Areas:

- Develop an **integrated approach to future undersea capabilities**

that coordinates platform, payload volume, payload, people and force posture plans; link the plan to require near term decisions or investments; take necessary actions to evolve tactical security in the face of anticipated threat improvements

- Outline the strategy to **continue to access, train, and retain the very best people that will fill our ranks**. This will require creative approaches to find and attract

the best and the brightest that the nation has to offer—people of character and integrity, technically skilled, with personal and leadership abilities.

- Define the **future role of undersea forces** to make best use of undersea concealment for national security, incorporating hedging strategies to accommodate uncertainty in global trends, technology and adversary's capability and intent

- Obtain SSBN, SSGN, SSN and Payload decisions to address SSBN requirements, SSGN replacement, the SSN force structure shortfall, and emergent payload requirements

Part III Detailed Discussion of Each Line of Effort

Ready Forces:

Providing Undersea Forces Ready for Operations and Warfighting Goals

1. Prepare undersea forces to safely and effectively complete peacetime operations directed by operational commanders. These operations will also support warfighting effectiveness.

2. Prepare undersea forces to effectively conduct wartime operations on short notice as directed by operational commanders.

3. Develop and refine, through experimentation, the command and control doctrine and TTP for the Undersea Warfare Commander for manned and unmanned systems.

In reaching these goals, our process must certify that the quality of provided forces meets standards. Furthermore, the process must be sustainable. It must not depend on shifting material and manpower excessively from one submarine to another in order to meet short-term commitments.

Ready Forces:

Focus Areas for increased emphasis

- **Enhance CO initiative and character**, responsibility, authority, and accountability to prepare the ship for operations and warfighting; structure the relationship with squadrons, groups and type commanders to shift the center of gravity for preparation, planning, execution, assessment and certification more to the ship; emphasize CO ability to distinguish acceptable risk from undue risk. Enhance CO effectiveness by nurturing integrity and a strong character at every opportunity.

- **Adopt a culture of sustained warfighting readiness** during the inter-deployment period; adjust the interaction within the chain of command to reward stable, broad excellence vice short-term, cyclic pulses; return tactical initiative to the operating forces.

Mindset: "This is the last week of peace before going to war."

- **Develop Undersea Warfare Commander Doctrine and TTP;** integrated

C2 for both manned and unmanned undersea systems; practices for effective coordination of mixed undersea forces with other forces.

Ready Forces:

Detailed Application of the Focus Areas

1. Personnel Readiness:

Improve the accession, training, and retention of our people. This will be done through Systematic Rating Deep Dives (FIT), Unplanned Losses (UPLs) Deep Dive, follow-up on Engineering Department Master Chief (EDMC) community corrective actions. Enhance Sailor and Family resiliency with a systematic approach to preparing our Sailors and their families for submarine duty responsibilities. Improve the effectiveness of the officer career training pipeline, providing a more coherent, career approach towards developing a submarine Commanding Officer—including more deliberate emphasis on the developmental role of sea tours.

2. Fleet Readiness and Training Plan (FRTP): Revise the FRTP to increase the amount of time available for the ship's Commanding Officer and ISIC to effectively train

their crews. Lengthen FRTP underway periods to increase stable, at-sea training time. Increase CO latitude in tailoring submarine schedules.

3. Training: Update the Continuing Training Manual (CTM) and Continuing Training Support System (CTSS) to provide COs more useful assistance on how to build a successful training program. (Examples: better planning tools, Force Exam Bank use, alignment of qualification and training, and better tracking in CTSS). While maintaining the predominantly human element in training, consider approaches to "distance support" for training, particularly in examinations. Establishing a predominantly watch-team approach to operational training.

4. Assessment:Provide an instruction that describes assessment as a means for improvement. Shift the emphasis from external (ISIC) "exam workups" in support of "snapshot" assessments, to developing and evaluating a submarine crew's ability to assess itself, correct and improve itself, and establish a mindset of sustained, broad superior performance. Adjust engagement at the ship, ISIC and TYCOM levels to focus on developing the mindset and behaviors for sustained performance, while shifting the center of gravity for assessment and improvement to the submarine and CO. As a supporting action, achieve a more "steady strain" approach to readiness by considering more unscheduled exams (e.g. TREs and ORSEs). Ensure that exams include an assessment of the "sustaining" mindset and behaviors on board the submarine.

5. Maintenance/Materiel: As we have throughout our history, we will set and achieve uncompromising standards of material readiness—our environment demands nothing less.

Intermediate Maintenance: Reduce lost operating days and degraded readiness due to maintenance schedule overruns by optimizing the planning and scheduling of maintenance periods within the FRTP and during refits. Manage transitions (first/last 100 hours) more tightly, emphasize planning, strict control of growth/new work and adherence to key events schedule.

Depot Maintenance: Control duration and cost by better planning and transition management. Work with NAVSEA to shorten SSBN ERO duration. Manage depot maintenance transition with rigor similar to deploying a ship. Forecast work package requirements via more accurate Technical Foundation Papers to enable proper Shipyard loading and resourcing. Work with NAVSEA to establish better execution and planning metrics.

Modernization: Focus modernization efforts to more concisely address improved human-systems interfaces and reduced training burdens while improving the capabilities and reliability of key sensors such as towed arrays and photonics masts. Better balance operational requirements, fiscal realities, and sustainability in the COTS strategy.

Supply: Improve sustainment and reduce cannibalization by better supply support (particularly Virginia class) and proactive management of onboard and off hull supply parts with NAVSEA and NAVSUP partners.

6. Develop Undersea Warfare Commander Doctrine: Formalize standardized doctrine and procedures for coordinating the operations and effects of the full range of undersea systems with special emphasis on incorporating unmanned undersea systems into broad Navy operations. Anticipate emerging changes in communications, networking and autonomous operations to keep TTP current.

Effective Employment:

Conducting Effective Undersea Operations and Warfighting Today

Goals:

1. Optimally employ our undersea forces independently or as part of a team in support of our operational or warfighting responsibilities.

2. Reliably and professionally accomplish the missions tasked by the operational commanders while effectively managing risk and stealth.

3. Upon direction, go to war and immediately execute the combatant commanders' direction.

This objective is about establishing undersea superiority at the time and place of our choosing through the optimum employment of undersea forces. It involves every element from the deliberate advanced planning of forward operations and SSBN patrols to the conduct of combat operations.

Effective Employment:

Focus Areas for increased emphasis

- Active engagement with Fleet and Operational Commanders to develop coordinated theater specific campaign plans that optimally employ our undersea forces; enhance development of innovative strategic and tactical employment of undersea forces (e.g., C7F Submarine Campaign Plan and supporting CSP Submarine Response Plan); tighten our assessment processes with Operational Commanders and supporting players to make us more effective warfighters.

- Increase the deliberate and planned demonstration of warfighting capabilities and access at the submarine and force level enhancing confidence in our abilities and systematically proving we can do what's required; lead in development of Theater USW Doctrine and teamwork; improve Mission Assurance to ensure we can fight through a range of C4I challenges in peacetime and war

- Improve operational availability of undersea forces while forward (through improved resilience, achieve, on-board repair, in-theater repair)

Effective Employment:

Detailed Application of the Focus Areas

1. Theater Specific Employment Planning—Submarine Campaign Plans:

Formally coordinate and proactively engage Fleet and Operational commanders to thoroughly understand theater OPLANs, required capabilities (including access) and gaps. Encourage creative employment of submarines and undersea assets to conduct forward operations that improve our warfighting readiness and take advantage of our full range of capabilities (e.g., SSGN). Working closely with operational commanders, build

a multi-year employment plan and theater-specific Submarine Campaign Plans. By necessity, plans must include solutions to warfighting in communications degraded environments. Integrate innovative demonstrations of undersea force employment or warfighting capabilities into deployments. Integrate capability development into the preparation of Ready Forces.

2. Operating Our Ships—Developing Confidence and Demonstrating Operational and Warfighting Excellence:

Exploit opportunities to enable COs and crews to operate in anticipated wartime areas, walk the battlefield, prove access and demonstrate warfighting skills and postures (e.g., operations in degraded C2/GPS, operational agility , application of wartime ROE, in-theater torpedo firings, SSBN patrols uninterrupted by “Brief Stops,” etc).

Systematically test and evolve guidance based on lessons learned and experience gained. Conduct entire deployments or patrols at heightened stealth postures; assess stealth in-situ with short notice planned events (e.g., P3, SECEX). Exploit real world and exercise opportunities to incorporate unmanned systems (aerial and underwater) into forward operations and warfighting demonstrations. Provide feedback to help evolve USW Commander Doctrine and better leverage the capabilities of our undersea platforms and supporting forces. Include COs in the development of operational orders including proposed tasking, identification of best practices and pitfalls, and required mission rehearsals. Increase attention to “calculated risk” versus “undue risk.”

3. Sustaining Our Advantage—Forward Materiel Availability: Sustain the availability of essential systems in forward areas by improved reliability, logistic support, at-sea repair capacity and back- up/redundant modes of operation. Increase expected availability of tenders in Phase 0 and wartime. Submarine sensors, antennas, DSE support equipment, fire control and weapons require improved forward availability, as does IUSS-related equipment. Improve forward ordnance availability. Demonstrate warfighting support such as in-theater reloading, at-sea resupply, remote site maintenance and other required skills.

4. Sustaining the Fight—Mission Assurance: Ensure our readiness to support the Operational Commander throughout a range of C4I challenges in peacetime and war.

Build on existing collaboration and coordination between Submarine Operating Authorities to ensure seamless undersea support to the warfighter. Review, assess, and improve Continuity of Operations Plans.

5. Assessing Our Performance—Feedback to Make Us Better: Establish tighter feedback to the submarine preparation process from operational commanders, other forces and the intelligence community regarding forward operations. Formally assess training doctrine, tactical development, tactical security, modernization plans, concepts of operation, system performance, and forward maintenance practices. Scrutinize Tier 2/3 events and formalize lessons-learned. Assess likely future warfighting environments and determine what is necessary for success and make the necessary adjustments across the Force.

Future Force Capabilities:

Preparing for Future Undersea Operations and Warfighting

Goals:

1. Define the future role of undersea forces in both operations and warfighting.

2. Determine platform, payload, payload volume, people and posture requirements.

3. Coordinate future missions with other warfare communities.

4. Translate requirements into decisions, policy and funding.

This area of effort deals with the future beyond the next five years and must take into consideration uncertainty about future projections. There are, however, some factors that can be reliably foreseen: by the existing program of record, the number of nuclear submarines will shrink by about 30 percent over the next 20 years. By 2030, our forward presence will decline by more than 40 percent and our undersea strike capacity will drop by almost 60 percent. Despite these trends, there is every reason to believe that the future

of naval warfare will place increasing, and not decreasing demands on undersea forces.

This divergence of resources and demands places ever greater stress on the importance of an integrated approach for our future undersea capability development.

Future Force Capabilities: Focus Areas for increased emphasis

- Define the future role of undersea forces to make best use of undersea concealment for national security, incorporating hedging strategies to accommodate uncertainty in global trends, technologies and adversaries

- Develop an Integrated Undersea Future Strategy to align requirements for platforms, payloads, payload volume, people and force posture

- Obtain SSBN, SSGN, SSN and Payload decisions to address SSBN requirements, SSGN replacement, the SSN force structure shortfall, and emergent payload requirements

Future Force Capabilities: Detailed Application of the Focus Areas

1. Future Role of Undersea Forces—Long Term Undersea Warfighting Vision: Create a clear and broadly accepted vision of the growing importance of undersea forces in a future with increasing anti-access area-denial (A2AD) systems. Refine Navy and Joint Force understanding of the importance of undersea concealment to maritime military success. Advocate the implementation of the "Concept for Leveraging the Undersea Environment." Highlight the distinction between A2AD defense, penetration and defeat.

2. Future Payload, Platform, Payload Volume, People and Posture –

Integrated Undersea Future Strategy:

Platforms: Determine requirements for OHIO Replacement SSBN and its impact on SSGN replacement. Determine requirements for SSGN replacement and implications on SSBNs and SSNs. Determine approach for dealing with the SSN shortfall after 2024 and how that impacts SSGN replacement options.

Payload Volume: Consider the merits of the Virginia Payload Module to replace lost payload volume (distributed vs. concentrated firepower). Plan to simplify payload interfaces.

Payloads: Enhance the military utility of existing payloads through incremental evolutionary changes without needing new programs. Plan to resume torpedo production.

Determine new payloads required and their impact on payload volume needs.

Consider future sonar system requirements. Conduct liaison with SOCOM to determine the way ahead for SOF payloads. Align payloads with evolving tactical security needs.

People: Determine system and payload changes (sonar, fire control, software, etc.) to enable reduced manning. Identify means to promote increased operational efficiency. Anticipate and define necessary new skill sets, then determine how best to recruit, train and retain them.

Posture: Identify the implications to future operations given different force levels, payloads, basing and manning schemes. Determine how best to operationally integrate diverse undersea systems, including UUVs, in the future. Refine the mission area of subsea warfare and the systems/operations needed to carry it out.

3. Long-term decisions, policies and funding—SSBN, SSGN, SSN and

Payload decisions:

SSBN: Attain decisions on the OHIO Replacement capabilities, including stealth, survivability, and sustainment model. Ensure long- term continuity of sea-based strategic deterrence.

SSGN: Attain decisions on replacement of SSGN capacity when SSGNs retire, including Virginia Payload Module R&D and procurement funding.

SSN: Attain and sustain two-per-year procurement of Virginia-class SSNs.

Gain support for extending the life of selected SSNs to help fill the SSN shortfall without impacting the plan for SSN replacement. Defer the "New SSN" while continuing

procurement of additional Blocks of VA-class SSNs with associated incremental enhancements until after completion of OHIO Replacement class procurement.

Payloads: Encourage the development of undersea payloads by other resource sponsors, including Conventional Prompt Global Strike (OSD), Large Displacement Unmanned Undersea Vehicles (LDUUV)(N2/N6), next generation SOF vehicles (SOCOM), and Distributed Netted Systems.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Caldwell, J. F., J.M. Richardson, and R.P. Breckenridge. July 2011. *Design for Undersea Warfare Initiatives.* Norfolk, VA.: Commander Submarine Force Atlantic Fleet.http://www.public.navy.mil/subfor/hq/PDF/Undersea%20Warfighting.pdf.

Cisco Incorporated. 2009. "Securing Unified CCE." Last modified August 18, 2009. http://www.cisco.com/en/U.S./docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/srnd/75/c7scurty.pdf.

Department of Defense Joint Publication: Department of the Army, Department of the Navy: United States Marine Corps, Department of the Navy, Department of the Air Force, and United States Coast Guard. 2013. Joint Publication 1–02, *Department of Defense Dictionary of Military and Associated Terms* (JP1–02). http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. Joint Publication 1–02.

Commander Submarine Force. October 31, 2011. "CYBER-1, *Cyber Security, Network Readiness, And Information Assurance Manual*." Norfolk, VA: Commander Submarine Force. Use

Commander Submarine Force Atlantic. February 8, 2013. *"Message Additional ITS Conversion Opportunities."* Norfolk, VA: Commander Submarine Force.

Commander Submarine Force Atlantic. February 8, 2013. "*Update on the Status of the ITS Community and Conversion Opportunities."* Norfolk, VA: Commander Submarine Force.

Dean, Tamara. 2013. *Network Plus Guide to Networks*. 6th ed. Boston: Course Technology Cengage Learning.

Department of Defense RMG. 2006. "*Risk Management Guide for DoD Acquisition* 6th Ed." http://www.acq.osd.mil/se/docs/2006-RM-Guide-4Aug06-final-version.pdf.

Defense Information Systems Agency. 2013. Information Assurance Support Information (IASE) Policy and Guidance. Last modified June 28, 2013. http://iase.disa.mil/policy-guidance/index.html#cnd.

Grimes, John G. 2012. "Information Assurance Workforce Improvement Program Networks and Information." Assistant Secretary of Defense for DoD CIO.

National Security Administration Information Assurance Symposium. August 27–28, 2012. Nashville, TN.

Labert, Matthew J. 2002. “Implementation of Information Assurance Risk Management Training into Existing Department of the Navy Training Pipelines.” Master’s thesis, Naval Postgraduate School.

Microsoft. 2013. “End-to-End Security.” Windows Server, Technet, Microsoft. Last modified March 28, 2003. http://technet.microsoft.com/en-us/library/cc738845(v=ws.10).aspx.

NIST 800–30 Rev1. 2012. “Guide for Conducting Risk Assessments.” National institute of standards and technology.

NIST 800–37. 2010. “Guide for Applying the Risk Management Framework to Federal Information Systems.”

NSA-IA, Group. 2013. “Defense in Depth.” National Security Agency :Information Assurance Solutions Group. http://www.nsa.gov/ia/_files/support/defenseindepth.pdfhttp://www.nstissc.gov/assets/pdf/4009.pdf .

Office of the Undersecretary of Defense. 2013. “CIO Support: Information Assurance.” Personnel and Readiness Information Management (P&R IM) Office of the Under Secretary of Defense (Personnel & Readiness). http://www.prim.osd.mil/cap/cio-ia.html.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. 2002. “Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology.” Gaithersburg.

Vena, Peter D. 1998. “Information Technology Competencies for Navy Enlisted Personnel.” Master’s thesis, Naval Postgraduate School.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California